# ICCOTWT 2020

09 & 10 July 2020

Michigan,
United States of America

ISBN: 978-93-88122-13-9

*Proceedings of the Fifth International Conference on Cloud of Things and Wearable Technologies 2020*

A S D F

SUBRA GANESAN

*International Conference on Cloud of Things and Wearable Technologies 2020*

# ICCOTWT 2020

# Volume 1

By
ASDF, North America

Financially Sponsored By
Association of Scientists, Developers and Faculties, India

Multiple Areas

## 09-10, July 2020

## Michigan, United States of America

*Editor-in-Chief*
**Subramaniam Ganesan**

*Editors:*

Daniel James, Kokula Krishna Hari Kunasekaran and Saikishore Elangovan

*Published by*

**Association of Scientists, Developers and Faculties**
Address: RMZ Millennia Business Park, Campus 4B, Phase II, 6th Floor, No. 143, Dr. MGR Salai, Kandanchavady, Perungudi, Chennai – 600 096, India.
Email: admin@asdf.org.in || www.asdf.org.in

## International Conference on Cloud of Things and Wearable Technologies (ICCOTWT 2020)

## VOLUME 1

Editor-in-Chief: **Subramaniam Ganesan**
Editors: **Daniel James, Kokula Krishna Hari Kunasekaran and Saikishore Elangovan**

**Disclaimer:**

No responsibility is assumed by the ICCOTWT 2020 Organizers/Publisher for any injury and/ or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products or ideas contained in the material herein. Contents, used in the papers and how it is submitted and approved by the contributors after changes in the formatting. Whilst every attempt made to ensure that all aspects of the paper are uniform in style, the ICCOTWT 2020 Organizers, Publisher or the Editor(s) will not be responsible whatsoever for the accuracy, correctness or representation of any statements or documents presented in the papers.

ISBN-13: 978-93-88122-13-9
ISBN-10: 93-88122-13-5

## TECHNICAL REVIEWERS

- Abdelrahman Elewah, Benha Faculty of Engineering, Egypt
- Abdulrazak Mohamed, School of Planning and Architecture, Vijayawada, India
- Abhishek Bajpai, Rajkiya Engineering College, India
- Achal Garg, Keppel Offshore and Marine, India
- Aede Hatib Musta'amal, Universiti Teknologi Malaysia, Malaysia
- Ahmed Mehany, Beni-suef University, Egypt
- Ahmed Mohamed, Beni Suef University, Egypt
- Ahmed Mohammed Kamaruddeen, University College of Technology Sarawak, Malaysia
- Alaa El-hazek, Faculty of Engineering At Shoubra, Benha University, Egypt
- Alagammal Mohan, Mepco Schlenk Engineering College, Sivakasi, India
- Ali Berkol, Baskent University, Turkey
- Allin Joe David, Kumaraguru College of Technology, India
- Ambavarm Vijaya Bhaskar Reddy, Universiti Teknologi Petronas, Malaysia
- Ambika Pathy, Galgotias College of Engineering College And Technology, India
- Ammar Jreisat, Al Ain University of Science and Technology, United Arab Emirates
- Amol Potgantwar, Sandip Institute of Technology & Research Centre Nasik, India
- Amr Helmy, The British University in Egypt, Egypt
- Anand Nayyar, Duy Tan University, Da Nang, Vietnam, Viet Nam
- Anbuoli Parthasarathy, Anna University, India
- Anil Dubey, Abes Engineering College Ghaziabad, India
- Aniruddha Thuse, Jgi's Jain College of Mba & Mca, Belagavi, Karnataka, India
- Anitha Natarajan, Kongu Engineering College, India
- Ankur Bist, Kiet Ghaziabad, India
- Anshul Garg, Taylor's University, Malaysia
- Appavu Alias Balamurugan Subramanian, E.G.S Pillay Engineering College, India
- Aravind C.k., Mepco Schlenk Engineering College, Sivakasi, India
- Ariffin Abdul Mutalib, Universiti Utara Malaysia, Malaysia

- Arockia Xavier Annie Rayan, Anna University, India
- Arshad Mansoor, Civil Defence, Riaydh, Saudi Arabia
- Arul Teen, University College of Engineering Nagercoil, India
- Arumugam Raman, Universiti Utara Malaysia, Malaysia
- Arun M R, SXCCE, Anna University, India
- Arun Sharma, Indira Gandhi Delhi Technical University for Women, Delhi, India
- Arun Pandian Jaya Pandian, M.A.M. College of Engineering and Technology, India
- Arupaddiyappan Sivasubramanian, V I T University, India
- Ashokkumar Nagarajan, Sree Vidyanikethan Engineering College, India
- Asokan Ramasamy, Kongunadu College of Engineering and Technology, India
- Ayyanadar Arunachalam, Indian Council of Agricultural Research, India
- Azwa Abdul Aziz, Universiti Sultan Zainal Abidin, Malaysia
- Bala Venkata Subrahmanyam, TKREC, India
- Balachandar Krishnamoorthy, Sastra Deemed to be University, India
- Balaji Kalaiarasu, Amrita Vishwa Vidyapeetham, Coimbatore, India
- Balakrishnan Kandasamy, Karpaga Vinayaga College of Engineering and Technology, India
- Balakrishnan Subramanian, Sri Krishna College of Engineering and Technology, Coimbatore, India
- Balamuralitharan Sundarappan, SRM IST, India
- Balamurugan N M, Sri Venkateswara College of Engineering, India
- Balamurugan Sivaramakrishnan, Coimbatore Institute of Technology, India
- Bhanu Prakash Kolla, Koneru Lakshmaiah Education Foundation, India
- Bhavani Anand, Mepco Schlenk Engineering College, India
- Bhavna Ambudkar, Dr. D.y Patil Institute of Technology, Pimpri, India
- C V Guru Rao Rajagopal Rao, Sr Engineering College, India
- Carlo Inovero, Polytechnic University of The Philippines, Philippines
- Chandrasekaran Muthial Chetty, Government College of Engineering, Bargur, Tamil Nadu, India
- Charles Weeraratna, Lanka Rainwater Harvesting Forum, Sri Lanka

- Chitra Krishnan, VIT Chennai, India
- Christopher Hill, The British University in Dubai, United Arab Emirates
- Dafni Rose, St. Joseph's Institute of Technology, India
- David Rathnaraj Jebamani, Sri Ramakrishna Engineering College, India
- David Wilson Devarajan, English/ Karunya Institute of Technology & Sciences, India
- Deepa Dhanaskodi, Bannari Amman Institute of Technology, India
- Deepa Jose, KCG College of Technology, India
- Deepa Rani T, India
- Deepali Sawai, Atss's Institute of Industrial and Computer Management and Research (IICMR), India
- Delampady Narasimha, Indian Institute of Technology Dharwad, India
- Devendra Kumar Rangasamy Natarajan, Sri Ramakrishna Institute of Technology, India
- Dharma Raj Cheruku, GITAM, India
- Diaa Salama, Faculty Of Computers and Informatics, Benha University, Egypt
- Dinkar Nandwana, Asm America Inc, United States
- Dishek Mankad, Shri P.K.M. College of Technology & B.Ed., India
- Djilali Idoughi, University A. Mira of Bejaia, Algeria
- Doha Tawfiq, Faculty of Agriculture, Benha University, Egypt
- Durata Haciu, KOC University, Turkey
- Edwin Christopher Samuel, Jain Group of Institutions, India
- Ela Kumar Kumar, IG, India
- Elvis Chabejong Nkwetta, Institut Fur Medizinische Informationsverarbeitung, Biometrie Und Epidemiologie, Germany
- Faten Kharbat, Al Ain University of Science and Technology, United Arab Emirates
- Fiorella Battaglia, Ludwig-maximilians-university, Germany
- G R Sinha, Myanmar Institute of Information Technology Mandalay, Myanmar
- Ganesan Ganapathy, Adikavi Nannaya University, India
- Ganesh Kumar P, K.L.N College of Engineering, China, India

- Geetha Mohan, Jerusalem College of Engineering, India
- Gnanajeyaraman Rajaram, Sbm College of Engineering and Technology, India
- Gnanasekaran Jekka Subramanian, K.L.N. College of Information Technology, India
- Gopirkishnan Sundaram, Karpagam Institute of Technology, India
- Govindasamy Vaiyapuri, Pondicherry Engineering College, India
- Gurumurthy Hegde, Centre for Nano-materials & Displays, BMS College of Engineering, India
- Hamid Al-asadi, Basra University, Iraq
- Hamid Behnam, Western Sydney University, Australia
- Hamzh Alalawneh, Fbsu/ Unisza, Saudi Arabia
- Hanumantha Reddy, Rao Bahadur Y Mahabaleswarappa Engineering College, Cantonment, Bellary, India
- Hao Yi, Northwestern Polytechnical University, China
- Hardeep Singh, Ferozepur College of Engineering & Technology (FCET), India
- Hariharan Vaggeeram, Kongu Engineering College, Erode, India
- Harikiran Jonnadula, Shri Vishnu Engineering College for Women, India
- Harikrishna Kumar Mohan Kumar, Kongu Engineering College, India
- Harikrishnan Santhanam, Adhi College of Engineering & Technology, India
- Hemanth Chandran, Vellore Institute of Technology Chennai, India
- Jagannath Mohan, Vellore Institute of Technology (VIT) Chennai, India
- Jagathy Raj V. P., Cochin University of Science and Technology, India
- Javier Dario Fernandez Ledesma, University Pontificia Bolivariana, Colombia
- Jayshree Sanjay Kumar Soni, JNVU, Jodhpur, India
- Jitendra Agrawal, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India
- Jitendra Singh, SRM University, India
- Jyothi Badnal, Chaitanya Bharati Institute of Technology, India
- Kala Iyapillai, SNS College of Engineering, India
- Kalaivani Anbarasan, Saveetha School of Engineering, India
- Kalpana Murugan, Kalasalingam Academy of Research And Education, India

- Kannan Gopal Radhakrishnan, PSNA College of Engineering and Technology, India
- Kannan Kilavan Packiam, Bannari Amman Institute of Technology, India
- Kareem Kamal A.ghany, Beni-suef University, Egypt
- Karthi Kumar Ramamoorthy, Kumaraguru College of Technology, India
- Karthik Subburathinam, SNS College of Technology, India
- Karthikeyan Jayaraman, Mangayarkarasi College of Engineering, Madurai, India
- Karthikeyan Parthasarathy, Kongu Engineering College, India
- Kavitha Kanagaraj, Kumaraguru College of Technology, India
- Kavitha R V R Venkatachalapathi, PES University, India
- Kiran Kumar Kudumula, Rajeev Gandhi University, India
- Kokula Krishna Hari Kunasekaran, Techno Forum R&D Centre, India
- Kolli Balakrishna, GITAM University Hyderabad Campus, India
- Krishnakumar Subbian, DRDO, India
- Kumaresan Jeganathan, Amrita Vishwa Vidyapeetham, India
- Latha Kesavarao, Anna University (BIT Campus), India
- Laura Dass, Universiti Teknologi Mara, Malaysia
- Liana Stanca, Babes-bolyai University, Romania
- Ma. Angela Leonor Aguinaldo, Max Planck Institute for Foreign and International Criminal Law, Germany
- Madhavi Tatineni, GITAM, India
- Makhlouf Mohamed Mahmoud Bekhit, Faculty of Agriculture, Moshtohor, Benha University, Egypt
- Malathi Raman, Annamalai University, India
- Malliga Subramanian, Kongu Engineering College, India
- Mallikarjuna Reddy, GITAM University, India
- Malmurugan Nagarajan, Mahendra College of Engineering, India
- Mani Veloor N, Centre for Materials for Electronics Technology, Govt. of India, India
- Manik Sharma, DAV University Jalandhar, India

- Manikandan Vairaven, Kalasalingam Acadamy of Research and Education, India
- Manish Bhardwaj, KIET Group of Institutions, India
- Manjula Devi Ramsamy, Kongu Engineering College, India
- Manoj Kumar Majumder, Dr. S. P. Mukhrejee International Institute of Information Technology, Naya Raipur, India
- Manusankar C, SSV College, Valayanchirangara, India
- Manvender Kaur Sarjit Singh, Universiti Utara Malaysia, Malaysia
- Marcia Pinheiro, IICSE University De, Australia
- Marikkannan Mariappan, Institute of Road and Transport Technology, India
- Marimuthu Nachimuthu, Nandha Engineering College, India
- Martin Sagayam Kulandairaj, Karunya Institute of Technology and Sciences, India
- Maslin Masrom, Universiti Teknologi Malaysia, Malaysia
- Mathivannan Jaganathan, Universiti Utara Malaysia, Malaysia
- Mathiyalagan Palaniappan, Sri Ramakrishna Engineering College, India
- Md. Haider Ali Biswas, Khulna University, Bangladesh
- Min Nie, Stevens Institute of Technology, United States
- Miroslav Mateev, American University in The Emirates, United Arab Emirates
- Missak Swarup Raju, GITAM Deemed to be University, India
- Mohamed Abd El-aal, Kanazawa University, Egypt
- Mohamed Abdo, Assiut University, Egypt
- Mohamed Ali, King Saud University, Saudi Arabia
- Mohamed Eid Shenana, Benha University, Egypt
- Mohamed Nayel, Assiut University, Egypt
- Mohamed Saleh, Harbin Institute of Technology, Egypt
- Mohamed Waly, Majmaah University, Egypt
- Mohammad Arif Kamal, Aligarh Muslim University, India
- Mohammed Ali Hussain, Kl University, India
- Mohammed Saber, Faculty of Engineering- Fayoum University, Egypt

- Mohd Helmy Abd Wahab, Universiti Tun Hussein Onn Malaysia, Malaysia
- Murali Muniraj, Sona College of Technology, India
- Murulidhar K S Shivaiah, K S I T, India
- Muthupandian Thangasamy, PSNA College of Engineering and Technology, India
- Muthuvel Arumugam, Sri Sairam College of Engineering, India
- Nagarani Suresh, Sri Ramakrishna Institute of Technology, India
- Navneet Agrawal, CTAE, MPUAT, Udaipur, India
- Nida Meddouri, Faculty of Mathematical, Physical and Natural Sciences of Tunis, Tunisia
- Nikhat Fatma Mumtaz Husain Shaikh, Pillai Hoc College of Engineering and Technology, Rasayani, India
- Nirmalkumar Krishnaswami, Kongu Engineering College, India
- Nisha Soms, Sri Ramakrishna Institute of Technology, India
- Noor Elaiza Abdul Khalid, University Teknologi Mara Malaysia, Malaysia
- Noor Raihani Zainol, Universiti Malaysia Kelantan, Malaysia
- Obaid Aldosari, Majmaah University, Saudi Arabia
- Omer Elmahadi, King Fahd University for Petroleum & Minerals, Saudi Arabia
- P.m.k. Prasad, GVP College of Engineering For Women, Visakhapatnam, India
- Panita Krongyuth, Sirindhorn College of Public Health, Ubon Ratchathani, Thailand
- Paramasivam Kuppusamy, Kumaraguru College of Technology, India
- Pethuru Raj Chelliah, Reliance Jio Infocomm Ltd., India
- Poongodi Chenniappan, Bannari Amman Institute of Technology, India
- Prabhakar Kollapudi, National Institute of Rural Development & Panchayati Raj (NIRDPR), India
- Prakash Subramanaiam, Sathyabama University, India
- Praveen Kumar Posa Krishnamoorthy, SVCE, India
- Puvaneswari Ganapathiappan, Coimbatore Institute of Technology, India
- Rabia Riad, Ibn Zohr University, Morocco
- Radhika Raavi, GITAM University, India
- Rafat Amin, Beni Suef University, Faculty of Science, Physics Department, Egypt

- Ragupathy Rengaswamy, Annamalai University, India
- Raj Mohan Radhakrishnan, Sastra Deemed University, India
- Raja Suzana Raja Kasim, Universiti Malaysia Kelantan, Malaysia
- Rajarajan Gopal, Hindustan Institute of Technology & Science, India
- Rajesh Keshavrao Deshmukh, S.s.i.p.m.t., Raipur, Chhattisgarh, India
- Rajesh Kanna Rajendran, Dr. N.G.P Arts and Science College, India
- Rajiv Kumar, Punjab Institute of Management and Technology, India
- Rajiv Selvam, Manipal University, India
- Rama Sree Sripada, Aditya Engineering College, India
- Ramasamy Pachaiyappan, Sri Balaji Chockalingam Engineering College, India
- Ramayah Thurasamy, School of Management/universiti Sains Malaysia, Malaysia
- Rames Panda, CSIR-CLRI, India
- Ramesh Balasubramanian, St. Joseph's Institute of Technology, India
- Ramesh Sengottuvelu, KCG College of Technology, India
- Rampradheep Gobi Subburaj, Kongu Engineering College, India
- Ramu Nagarajapillai, Annamalai University, India
- Rana Alabdan, Majmaah University, Saudi Arabia
- Randa Alarousy, National Research Center, Egypt
- Ravi Gulati, Veer Narmad South Gujarat University, India
- Ravikumar D.v., Adithya Institute of Technology, India
- Raviraj Pandian, GSSS Institute of Engineering & Technology for Women, India
- Rehab Nady, Faculty of Science - Beni-suef University, Egypt
- Reyhan Alhas, Mcmp/lmu Munchen, Germany
- Reza Gharoie Ahangar, University of North Texas, United States
- Roselina Sallehuddin, Universiti Teknologi Malaysia, Malaysia
- Ruchi Tuli, Jubail University College, Saudi Arabia
- Rupesh Dubey, IPS Academy Institute of Engineering & Science Indore, India
- S. Balamurugan, Quants Is & Cs, India

- S.V. kogilavani Shanmugavadivel, Kongu Engineering College, India
- Sabanayagam Angamuthu, Karpagam Institute of Technology, India
- Sadhik Basha J, International Maritime College Oman, Oman
- Sahar Badawy, Bue, Egypt
- Saikishore Elangovan, ,
- Saleh Altayyar, King Saud University, Saudi Arabia
- Sallehuddin Muhamad, Universiti Teknologi Malaysia, Malaysia
- Sandeep Bhat, SIT, Mangaluru, India
- Sangeetha Rengachary Gopalan, VIT University, India
- Sanjay Ghandhyambhai, LDRP-ITR, India
- Sanjay Kumbhar, Rajarambapu Institute of Technology, India
- Sanjay Pande, GM Institute of Technology, India
- Santhosh Kumar Balan, GMR Institute of Technology, India
- Sasikala Ramachandran, Kongu Engineering College, India
- Sasikala Senthamarai Kannan, Paavai Engineering College, India
- Sathish Babu, Department of Electronics and Instrumentation, India
- Sathish Gandhi Chinnasamy, University College of Engineering Nagercoil, India
- Sathish Kumar Nagarajan, Sri Ramakrishna Engineering College, Coimbatore, India
- Satish Sajja, V R Siddhartha Engineering College, India
- Sayed Gomaa, Al-azhar University and British University, Egypt
- Selvakumar Muthusamy, Sri Venkateswara College of Engineering, India
- Selvaperumal Sundara, Syed Ammal Engineering College, India
- Selvi Rajendran, KCG College of Technology, India
- Selvi Shanmugam, Institute of Road and Transport Technology, India
- Senthilkumar Kandasamy, Kongu Engineering College, India
- Senthilnathan Nattuthurai, Kongu Engineering College, India
- Shamsiah Banu Mohamad Hanefar, University of Nottingham Malaysia, Malaysia
- Shanmugapriyan Thiagarajan, ASDF International, India

- Shanmugasundaram O.l Lakshmanan, K.S. Rangasamy College of Technology, India
- Shanthakumari Raju, Kongu Engineering College, India
- Shanthi Radhakrishnan, Kumaraguru College of Technology, India
- Shekhar Ramaswamy, Alliance University, India
- Shidaling Matteppanavar, JNCASR Bangalore, India
- Shikha Maheshwari, JECRC, Jaipur, India
- Sivakumar Vaithilingam, Ramco Institute of Technology, India
- Sivaprakash Chokkalingam, Sri Sairam College of Engineering, India
- Sivaraja Muthusamy, N.S.N. College of Engineering and Technology, India
- Soonmin Drho, Inti International University, Malaysia
- Sreenivasa Rao Ijjada, GITAM University, India
- Sri Devi Ravana, University of Malaya, Malaysia
- Srinivasan Natrajan, Kongu Engineering College, India
- Subramaniam Ganesan, Oakland University, United States
- Subramanian Krishnamurthy, IGNOU/IIT, India
- Sudhakar Radhakrishnan, Dr. Mahalingam College of Engineering and Technology, India
- Sukamal Sanhita Deb, IGNOU, India
- Sukumar Ponnusamy, Nandha Engineering College (Autonomous), India
- Sundar Ganesh Chappani Sankaran, PSG College of Technology, India
- Sunita Daniel, Amity University Haryana, India
- Tamilarasi Angamuthu, Kongu Engineering College, India
- Tamilsalvi Mari, Taylor's University, Malaysia
- Tamilselvan K.s., Kongu Engineering College, India
- Tamizhselvan Perumal, Tamil Nadu Institute of Urban Studies, India
- Thamizhmaran Krishnamoorthy, Annamalai University, India
- Thangagiri Baskaran, Mepco Schlenk Engineerng College, India
- Thangamani Murugesan, Kongu Engineering College, India
- Thangavel Murugan, Thiagarajar College of Engineering, India

- Thangavel Subbaiyan, National Institute of Technology Puducherry, India
- Thenmozhi Rayan, Dayanandasagar College of Engineering, India
- Thilagamani Sathasivam, M. Kumarasamy College of Engineering (Autonomous), India
- Thirugnanam Gurunathan, Annamalai University, India
- Udhayakumari Duraisamy, Rajalakshmi Engineering College, India
- Uthirakumar Periyayya, Sona College of Technology, India
- Vadlamudi Parthasarathi Naidu, CSIR-national Aerospace Laboratories, India
- Valmiki Ramakrishna, Tumkur University, India
- Vasuki Arumugam, Kumaraguru College of Technology, India
- Vasunun Chumchua, Mahidol University, Thailand
- Veeraswamy Ammisetty, St.Ann's College of Engineering & Technology, India
- Venkata Subba Reddy Imma Reddy, GITAM (Deemed to be University), India
- Venkatanarayanan P.S., Hindustan Institute of Technology and Science, India
- Vijay Gupta, IITM, India
- Vijaya Deshmukh, National Institute of Fashion Technology, India
- Vijaya Kumar Y, Sri Sairam College of Engineering, India
- Vijaya Kumari Valsalam, Er.perumal Manimekalai Engineering College, India
- Vijayachitra Senniapppan, Kongu Engineering College, Perundurai, India
- Vijayan Gurumurthy Iyer, Koneru Lakshmaiah Education Foundation (KLEF), India
- Vijayaraja Kengaiah, KCG College of Technology, India
- Vikrant Bhateja, SRMGPC, Lucknow, U.p., India
- Vimala Vishwanath Achari, Avinashilingam Institute For Home Science and Higher Education for Women, Coimbatore, India
- Vinod Kapse, Gyan Ganga Institute of Technology and Sciences, Jabalpur, India
- Vipin Jain, Teerthanker Mahaveer University, India
- Visweswara Rao Pasupuleti, Universiti Malaysia Kelantan, Malaysia
- Vivekanandan Nellaiappan, Central Water and Power Research Station, India
- Vo Ngoc Phu, Duy Tan University, Viet Nam

- Walid Abdalhalim, Beni-suef University, Egypt
- Wan Hussain Wan Ishak, Universiti Utara Malaysia, Malaysia
- Xuan Wang, Utrgv, United States
- Yerra Rama Mohan Rao, Dr. Paul's Engineering College, India
- Yousef Farhaoui, Moulay Ismail University, Morocco
- Yousef Okour, Majmaah University, Saudi Arabia
- Yudi Fernando, Faculty of Industrial Management, Universiti Malaysia Pahang, Malaysia
- Zahira Rahiman, Tagore Engineering College, India
- Zahurin Samad, Universiti Sains Malaysia, Malaysia

# Table of Contents

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 24 June 2020 |
| Article ID | iccotwt.2584 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 01 July 2020 |
| eAID | 2020.iccotwt.2584 |

# AUTOMOTIVE DOMAIN CONTROLLER

**Dingwang Wang[1], Subramaniam Ganesan [2]**

[1,2] *Oakland University, Rochester, MI USA.*

**ABSTRACT**: Today, every electronic control system in the car, such as Instrument Cluster, Infotainment, Anti-lock braking system, Engine Management System, Transmission Control Unit, and Body Control Management is a self-sufficient unit with its own sources like ROM, RAM memory, microprocessor or microcontroller, I/O and power supply. The idea of automotive domain controller is to replace multiple distributed ECUs with a single powerful central computer with multi-core. Multi-core processing technologies integrate multiple ECUs into one single chip. In a multi-core solution, these individual ECUs retain separated and independent processing space. However, a lot of redundant components like housing, drivers, wire and harnesses, and power supplies can be eliminated. These not only largely save cost but also the component's weight and space. Moreover, communication between ECUs is within the processor itself instead of communicating over an external network like CAN or LIN, this will reduce the data latency and system complexity considerably.

**Keywords**: ECU, Domain controller

## I. INTRODUCTION

There are these following major reasons why we need Automotive Domain Controllers.

First, the current vehicle electric/electronic architecture integrates one or a few function features in every individual control unit. This increases not only the number of control units and distributed software functions but also the complexity of connectivity respectively. If there is a new feature is required to a car, to add one more new dedicated ECU and a little wire and harness is the common solution. There are already up to 70 dedicated ECUs from different suppliers are installed in a state-of-the-art midsize car, it is hitting the limits. Adding a new ECU for every new feature is no longer sustainable.

***Cite this Article as:*** *Wang, D., & Ganesan, S. (2020). AUTOMOTIVE DOMAIN CONTROLLER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (1st ed., Vol. 1, pp. 1-9). London, GB: ASDF International.*

Second, Automotive domain controller's technology is an irresistible trend for future automotive industry, it is fundamental for future cars to keep up with rapid technological changes. The demand to have more and more safety and software-oriented features is increasing at an unprecedented rate. All these need to increase the computing horsepower accordingly. Just like the latest iPhone has to add more computing power to run all the new functionality features, we have to add more computing horsepower in the vehicle to run all the desired new features. The current architecture approach is no longer viable to support the high speed data exchange and complex software algorithms, there is no enough computing power to meet the increasing growth requirement in content and complexity, and network infrastructure cannot support the data bandwidth and speed for the future. Additionally, the average age of a modern vehicle is more than 10 years which is much longer than Smartphone, and the automotive technologies are developing at an unprecedented rate. Vehicle owners increasingly expect to have Smartphone-like upgradability. They no longer accept if functionality and features remain unchanged through the whole vehicle's lifespan as we do now. However, all the features and functions in today's distributed ECUs have to be designed and implemented prior to vehicle launching. Over-The-Air updates technology is critical need for future vehicles. OTA updates can be used to provide new features and technologies, upgrade the existing functionality, patch bugs, and improve performance. These updates can avoid vehicle recalls and reduce customer warranty costs. As cars become more software dependent, the need of OTA updates is becoming more critical. In order to accomplish all these goals, we need more computing performance, embedded memory capacity and higher connectivity bandwidth, only the new vehicle architecture with Domain controllers can meet these requirements, it allows adding functions that are not available when the vehicle is launched.

Third, thanks to the availability of higher-performance automotive class systems on a chip (SoCs), and with the cost prices of SOC cost are dropping sharply these years and getting closer and closer to the traditional MCU prices. This is another motivation for automakers to integrate multiple functions on a domain controller.

## II. THE BENEFITS OF AUTOMOTIVE DOMAIN CONTROLLERS

Compared to the traditional dedicated ECUs, Domain controllers have the following major advantages.

### A. *Reduce weight and improve efficient*

Adding a new ECU and some wiring and harness for every new feature results in the wiring loom becoming the second heaviest component in the car just behind the engine. This trend does not conform to another lightweight design rule to improve energy efficiency and enhance the vehicle cruise range. The Domain controller can eliminate a number of redundant components like PCB, housing, power supply, wiring and harnesses. Take the automotive cockpit controller as the example, which combines and replaces the traditional instrument cluster, infotainment system, and HUD display, the whole system mass can be reduced by more than 30 percent.

### B. *Cost*

Adding a new ECU for new features is not sustainable any more. Dedicated MCUs, memories, power supply, PCB and other electronic components for the new ECU will significantly increase cost. And with the price of SOC with strong computing power is persistently falling, take the integrated cockpit solution as the example again, it can save at least $70 per vehicle as estimated.

### C. *Data latency*

Autonomous vehicles and safety features will need to receive and process massive data from environmental sensors and outside sources like other vehicles, infrastructure and cloud-based sources. All these data must be processed in real-time or very close to real-time which will require high performance computing power and high bandwidth network communication to minimum data latency [1]. Since the data will only be processed once in the domain controller with higher performance computing capability, rather than using a lot of microcontrollers and the data can be shared among different cores internally instead of communicating through different networks.

### D. *Upgradability*

As we move vehicle from mechanical to a digital platform, the importance of software has greatly grown and the average software lines of code have been increased exponentially. So the snowballing complexity is causing more and more software-related quality issues and vehicle recalls [2]. So over-the-air updates will become key capability to maintain and upgrade complex software. As cars' software has been decoupled from the hardware, it makes easier to upgrade the system.

### E. *Connectivity*

Thanks to the high-performance computing power and high-bandwidth communication that Domain controllers have, the driver will be connected with the external environment around them through digital platform and 5G Cellular network. Vehicle-to-Vehicle, Vehicle-to-Infrastructure, and Vehicle-to-Cloud technologies will allow the vehicle to communicate with other vehicles and surrounding like weather, traffic, road condition, traffic lights, updated maps, etc. All these data and information must be communicated and processed in real-time which will require high-bandwidth communication and high-performance on-board computing power. Obviously, the traditional discrete MCUs have no capability to support these technologies.

## III. Automotive Domain Controllers Design

IT and consumer electronics technologies can be transferred to the automotive field. Most technologies that we desire for Automotive domain controllers like SOC, embedded operating system, Hypervisors, Ethernet, and Over-the-Air updates are mature technologies, and have already been widely used in consumer electronics and other fields. Automotive domain controllers will benefit from IT and consumer electronics. However, there are still some technologies need to reinvent so that they meet the stringent automotive standards and higher consumer demands [3]. The demand for safety, security, performance, and usability leads the highest expectations of quality and reliability, which in consumer electronics are not the big concerns [3]. Automotive Electric and Electronics Architecture and Automotive function safety and security will become critical success factors and be discussed in this paper.

### A. *Architecture*

Architectures for future automotive electronics are quickly innovating. The safety features and autonomous driving demand higher computing performance and higher-bandwidth communication. In order to support connectivity and infotainment, the vehicles are expected to be transformed into a distributed IT system with cloud access; remote software updates; and high-bandwidth access to digital map, other vehicles, and the surrounding infrastructure [3].

Fig. 1 shows the future automotive E/E architecture, it needs to be able to scale across different segments and across different functional content, and can provide the means to manage and control the growing functional complexity and content, the architecture also needs to cope with change demands and expectations over time, it is expected to provide OTA updates to update or upgrade existing vehicles.

The updatability and upgradability of the architecture can increase the overall evolution speed and control after original sale. Separation of software and hardware benefits functional content largely independent from hardware and greatly improves the system scalability.

#### *1)* Characters

Service-Oriented Architecture: SOA approach has been widely applied in IT and consumer-electronics. SOA provides substantial abstracted interfaces for the overall system, its encapsulation allows system design and testing by using agile methods, and it can reduce the increasing complex and makes it easier to reuse software components between vehicles generations.

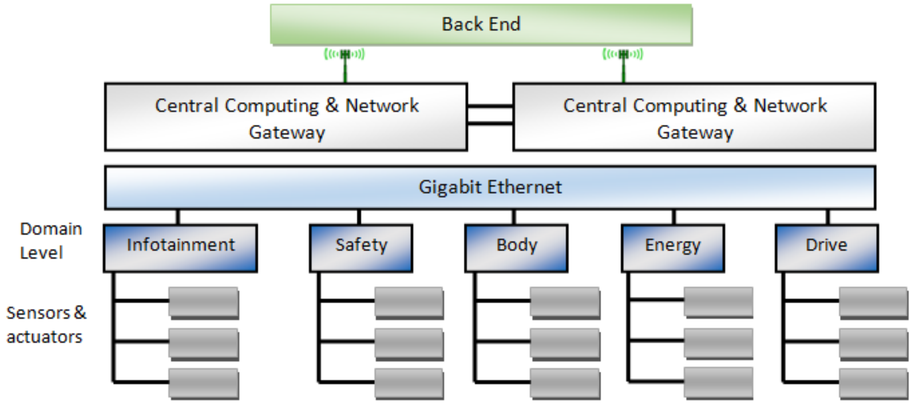


Fig. 1. Automotive E/E architecture for Domain controllers

### *a)* Central Gateway Server

A central information server and a broker will deal with all communication information. It isolates the local Domain controls from the external environments to maintain their safety and security.  The physical, information, and service will be separate. This benefits the extensibility and scales with less variance from a basic vehicle up to a fully equipped vehicle.

The central gateway in future automotive architecture serves as the information bridge to exchange information and isolate the in-vehicle domain controllers and peripheral communication sources like mobile cellular, Bluetooth, Wi-Fi, Ethernet. It also serves as the car's central diagnostic interface. The domain controllers also serve as the gateway between the central gateway and local smart sensors, actuators, and ECUs, to translate and exchange message between Ethernet and CAN or LIN.

The central gateway will take the main responsibility to maintain the network security. The central gateway verifies communications are coming from an approved source and protects authentications from being spoofed, and restricts network communications to predefined normal behavior and constrains abnormal or volumes of messages to avoid impairing the vehicle's functions. It also needs to block unapproved and inappropriate messages, and alert any invalid attempts. This can greatly improve the overall vehicle network security and significantly reduce the security burden of in-vehicle domain controllers.

### *b)* In-vehicle and back-end architectures

There is more and more interaction between in-vehicle systems and the back-end architecture. It will be connected via Wi-Fi, and high-bandwidth 5G cellular network. For safety features and autonomous control, vehicles will be required to exchange data and information with outside sources such as other vehicles, infrastructure and cloud-based sources, with information about weather, traffic, road construction, updated maps. Because it's not easy reprogrammed algorithms were not able to deal with and make the decision in real time for every possible scenario and changing driving conditions, more and more automotive functions need acquire data and information with the back-end systems and execute partly on the back end.

## *B.* Functional safety and information security

Functional safety is about ensuring the safe operation of systems even when they go wrong. Each industry typically has a standard to guide developments and set minimum expectations, and for automotive electronics it is ISO 26262, which defines functional safety as: the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical /electronic systems.

In practice, functional safety means a system that is demonstrably safe to an independent assessor in accordance with the target standards. Safety requires predictable failure modes which could be with full functionality, graceful degradation in functionality or clean shutdown followed by a reset and restart.

With the increasing in use of data connections and in-vehicle communication have made vehicles vulnerable to cyberattacks. The combination of increased electronic complexity and integration with other external components like keyless entry, Bluetooth, USB, telematics, wireless communications has provided portals into the control systems that are already deeply embedded in the vehicle.

Automotive computer security is used to detect, protect, and correct identifiable or avoidable threats and protect vehicles system from previously unknown or unavoidable ones. The collaborative approach includes hardware-based protection in and around the ECUs, software-based in-vehicle protections, network monitoring and enforcement in the vehicle.

There are many security strategies and knowledge available from the computer industry that can apply in automotive field. These include:

**Secure boot**: Software bootloader works with hardware to ensure that the loaded software codes are valid to provide a root of trust for the rest of the system [4].

**Partitioned operating system**: To isolate different applications or functions by using embedded operating system virtualization and partition techniques. This greatly reduces the complexity of consolidating multiple function systems onto one single SOC. This also makes it possible to update or refresh one individual features without affecting any other components [4]. And the overall operation will not be affected if one single module fails or crashes.

**Authentication**: Authentication is the process of verifying the identity of the sender of the data. For an embedded application, authentication is used to verify the source of data transmitted through external interfaces between different ECUs or SOCs. It also can be used to confirm the trustworthiness of a software image prior to executing it at run time, or during download from one external memory storage. In practice, electronic keys, passwords, and biometrics are needed to be managed and authorized to access some important information like identify, phone book, locations, and financial transactions. Similarly, the various ECUs or SOCs in the car also need to authenticate to prevent an attacker from faking messages or commands.

Enforcement of approved and appropriate behavior: In order to prevent cyber-attacks from trying to send messages from one system to another component, we need to detect and correct accidental or malicious threats [4].

## IV. Application and Discussion

### A. *Domain controller example --Infotainment domain controller*

Traditionally, we have at least two dedicated ECUs to handle instrument cluster information display, Head Up Display (HUD), and infotainment system separately as shown in Fig. 2. They have their own PCBs and packages and connect via CAN and MOST to exchange some vehicle information like speed and fuel range, and some infotainment information like phone book, navigation and media.

For infotainment domain controller as shown in Fig. 3, we are using one centralized controller to replace these two infotainment domain controller block diagram is illustrated as below.

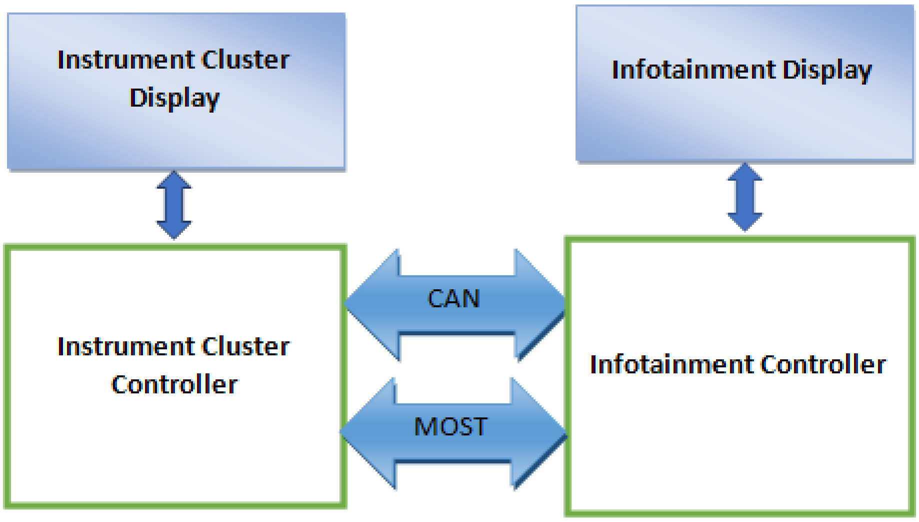


Fig. 2. Traditional infotainment system block diagram

This infotainment domain system as shown in Fig. 4 includes several displays under one common system architecture and Human-Machine interface. The display information content is no longer assigned to a dedicated display. All the display information is handled by the centralized controller and they can communicate within the processor to exchange the vehicle and infotainment information itself instead of communicating over an external network such as the CAN bus, increasing speed and reducing complexity. All information is flexible and can be display in the instrument cluster, head-up display, central display or even on a connected terminal like Smartphone depending on the driving situation. This greatly improves the flexibility and reduces the latency. Furthermore, they can share and reuse tremendous basic software like CAN, LIN, UART, Timer, A/D sample, HMI and so on, this considerably save the memory space and computing power, this also significantly reduce in the amount of software that must be developed and validated.

Renesas R-Car H3 SOC is chosen as the central computer for our infotainment domain controller, it has 4 cores and memory from 512M DDR3L to 4G LPDDR4, CPU and memory bandwidth can be scaled. We use third party embedded operating system QNX Hypervisor to partition, separate, and isolate safety-related environments from non-safety environments reliably and securely. The system equips Ethernet network to connect with external components and cloud. It is upgradeable over the air and will eventually communicate via 4G to the cloud. We can run both instrument cluster and infotainment applications with different safety and security requirements on this single hardware and software architecture platform. In order to keep pace with the consumer electronics and market dynamics, the infotainment feature has comparatively short life than instrument cluster's, this is also make it possible to only update dedicated software functions for infotainment sector. The safety-related driver information and long-lasting functions remain unaffected meantime. This approach has enough processing power and flexibility to add features in the future that don't exist today. Above all, this system solution can offer Flexible Modular Redundancy, if one core or application crash, other cores and application will not be affected, but rather can work as redundancy to replace.

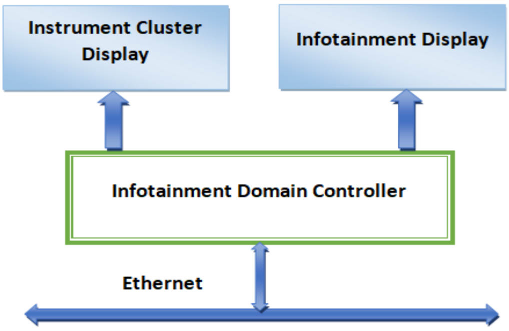


Fig. 3. Infotainment domain controller system block diagram

### B. *Major merits measurement*

Infotainment module consolidation is a technical trend to operate multiple traditional ECUs Instrument cluster and Infotainment by using modern, multi-core processor. The domain controller can eliminate a number of redundant components like PCB, housing, power suppliers, wire and harnesses, as well as the ECUs themselves. Additionally, ECUs exchange data within the processor itself instead of communicating over an external network like CAN or LIN bus, this will greatly reduce data latency and system complexity. Despite domain controllers have more functions safety and network security concern, while there is some merit to this concern including remote software upgradability, connectivity and flexibility. The major merits comparison between infotainment domain controller and dedicated ECUs are illustrated in Table I below.

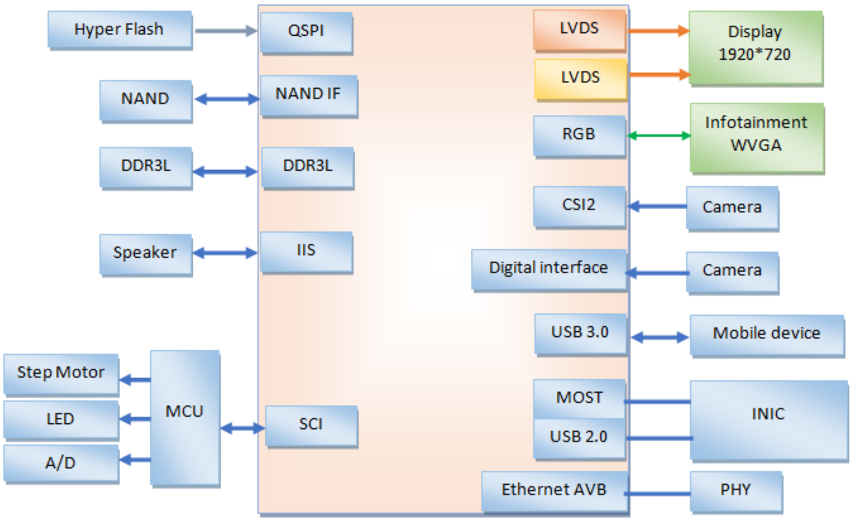


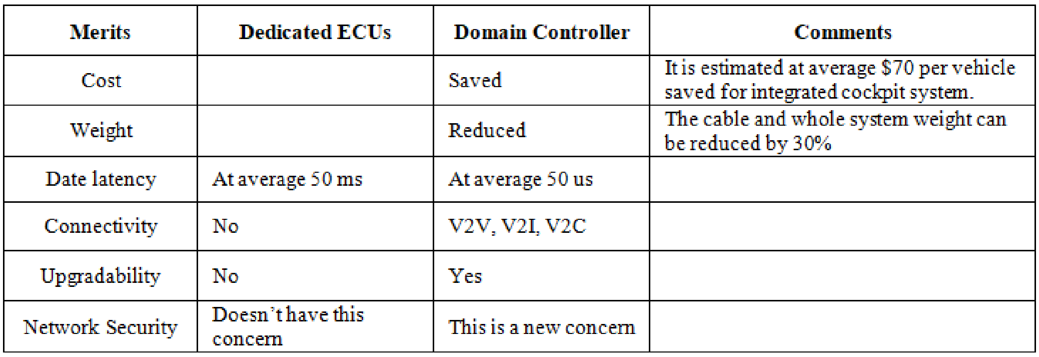
Fig. 4. Infotainment Domain controller Block Diagram

*Cite this Article as:* *Wang, D., & Ganesan, S. (2020). AUTOMOTIVE DOMAIN CONTROLLER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (1st ed., Vol. 1, pp. 1-9). London, GB: ASDF International.*

## V. CONCLUSION

Consumer demand for safety and software-oriented features is increasing at an unprecedented rate. The trend is shifting from distributed electronic controller units (ECUs) to more integrated domain controllers with centralized ECUs. Of course, this needs especially high demands on both the computing power and data memory size. However, the new vehicle architecture with domain controllers will deliver a fast, safe and reliable distribution of data and power. The new vehicle platform with domain controllers can easily take advantage of the state of the art from consumer electronics like cloud computing, internet connectivity and over-the-air software updates. Obviously, the powerful processors with multi-core, professional embedded operating system supports visualization, the innovational automotive architecture and high bandwidth Ethernet are the four major fundamental elements to achieve automotive domain controller concept.

TABLE I. MERITS COMPARISON



| Merits | Dedicated ECUs | Domain Controller | Comments |
|---|---|---|---|
| Cost | | Saved | It is estimated at average $70 per vehicle saved for integrated cockpit system. |
| Weight | | Reduced | The cable and whole system weight can be reduced by 30% |
| Date latency | At average 50 ms | At average 50 us | |
| Connectivity | No | V2V, V2I, V2C | |
| Upgradability | No | Yes | |
| Network Security | Doesn't have this concern | This is a new concern | |

## REFERENCES

[1] Mentor--Democratized autonomous vehicle system design.

[2] drej Burkacky, Johannes Deichmann, Georg Doll, and Christian Knochenhauer--Rethinking Car Software and Electronics architecture.

[3] 2017 Matthias Traub ; Alexander Maier ; Kai L. Barbehön-- Future automotive.

[4] McAfee – Automotive Security Best Practices

***Cite this Article as:*** *Wang, D., & Ganesan, S. (2020). AUTOMOTIVE DOMAIN CONTROLLER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (1st ed., Vol. 1, pp. 1-9). London, GB: ASDF International.*

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 25 June 2020 |
| Article ID | iccotwt.2612 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 02 July 2020 |
| eAID | 2020.iccotwt.2612 |

# HYBRID 3D METAL PRINTING

**Pavel Ikonomov**
*Western Michigan University, Kalamazoo, MI*

**ABSTRACT:** The goal of this research is to design, build, and test a novel and unique Hybrid 3D metal printer technology system employing both additive and subtractive processes in one unit. The system is capable of producing a high quality finished components on one setup. The Hybrid 3D metal printer technology is an integration of control and physical systems of Gas Metal Arc Welding (GMAW) unit used for material deposition and a Computer Numerically Controlled (CNC) milling machine used for material removal. This system provides a smaller footprint and a more cost-effective way to produce complex metal parts than other competitive 3D metal printing technologies. Both 3D metal printing and machining are digitally controlled from a computer program using a standard digital interface utilizing CNC programming. As a supplementary benefit, the proposed Hybrid 3D metal printer is user-friendly; a user without additional experience than CNC machining can produce functional, high-quality products.

**Keywords:** Three dimensional printing, hybrid metal printing, additive manufacturing, CNC machining

## 1. INTRODUCTION

### 1.1 Background

The most common 3D (three dimensional) printing technology (also known as Additive Manufacturing) has been developed around plastics and is still a relatively new technology. While there are many options

***Cite this article as:*** *Ikonomov, P. (2020). HYBRID 3D METAL PRINTING. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

of equipment like one used in the airspace and jet propulsion industries [1].

Presently there are two fundamental 3-D metal technologies to build a part layer-upon-layer. Laser sintering of metal powder and direct metal deposition using laser/high energy beam to melt powder on a metal substrate, to create a part layer-by-layer. Parts made with either technique require using of support material to fabricate complex structures (overhang, bridges), secondary operations (follow on machining to achieve part tolerance and surface finishes), and additional labor to make the final product. The high cost of equipment and material, size limitations, maintenance and operation cost, and the extra added cost for secondary machining and finishing operation limits their application to low volume, high-cost parts used in industries like airspace [2, 3, 4]. These high-capital and operating costs of present 3D metal printing technology prevent many manufacturers from adopting it.

There are few hybrid 3D metal printing systems based on CNC manufacturers like DMG MORI, ELB-Schliff, Matsuura, Mazak, Mitsui Seiki, and Okuma and several new ones such as Diversified Machine Systems, Fabrisonic, and Optomec [4, 5].

Other companies such as Hybrid Manufacturing Technologies (HMT) and 3D-Hybrid Solutions, Inc. also provide add on solutions to CNC machines. Most of the 3d metal printing systems are based on laser sintering or direct metal deposition to create a 3D printed part at first, and then they are machined on the same or different equipment. Only a few systems use GMAW (also known as MIG- metal inert gas) welding for deposition, similar to our process [3, 4, 5]. Essentially, both groups metal powder and hybrid technologies completed the 3D printed parts first and machined them after that. These technologies pose several disadvantages with performance, quality, and cost. The cost of the machine, material, and maintenance is prohibitively high (starting from several hundred thousand to millions of dollars), and performance speed is quite low. Both groups could not produce complex overhang geometry without the support structure and provide in-situ layer control of building geometry, and surface finishes when machining each layer. We believe our system has several unique advantages in comparison with other technologies. It is capable of producing high-quality functional parts, with complex geometries, tight tolerance, and superior finish on the same machine while providing lower material and operation costs.

### 1.2 Additive and subtractive manufacturing

At present 3D printing, now called additive manufacturing (AM), is one of the fastest-growing manufacturing systems. The widespread became the usage is simple. It is often called 3D printing, implying that it is an extension of the 2D printing in one more dimension to produce 3D objects. Additive manufacturing is a type of so-called 3D printing process when a material is added layer by layer to build a 3D structure. We will explain this general process to reveal the difference with the proposed system described later. The explosive increase of the 3D printer usage is based on the fact that everybody, without any engineering knowledge, can produce their object, at relatively low cost, anytime at any place, and mostly at home. Another factor for extensive usage is that the AM type 3D printers and materials costs became very affordable.

### 1.3 Proposed 3D Metal Printing/Machining

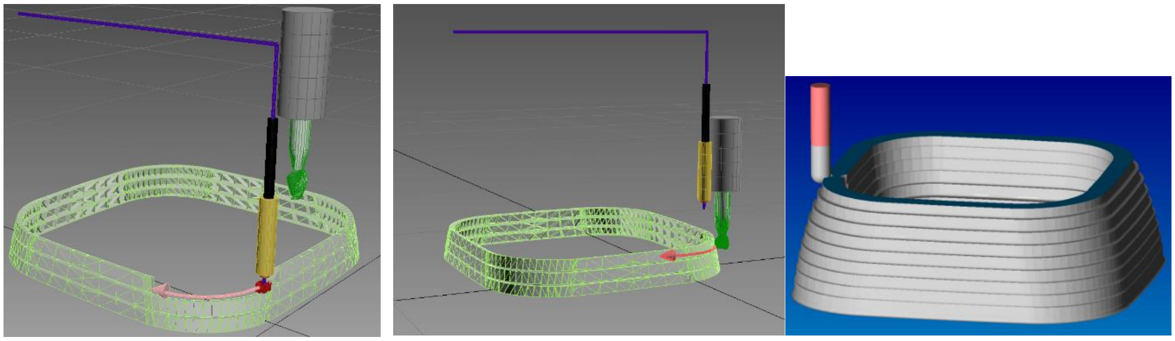
Traditional AM has many limitations, such as materials, mostly plastics, small working volume, and low quality, which could not even get closer to industrial quality products. Looking at the advantages and limitations of AM and subtractive manufacturing processes, we developed a new method to take the best of both processes without drawbacks. To distinguish our process from traditional AM and subtractive manufacturing (mostly metal cutting), we call our system Hybrid 3D metal printing that combines both methods.

Earlier research and knowledge are readily available to 3D metal printing materials and successfully applied in industry. There are many examples of successful applications of 3D metal printing like aircraft parts, Airbus titanium pylon bracket [6], engine parts by Mercedes [7], and WV [8], and Metal Jet fuel nozzles by GE [9]. Our hybrid 3D metal printer allows the building of additive/subtractive machines based on existing well-know and developed technologies GMAW welding and CNC machining, to deliver finished, ready to use parts, [10]. It can extend the existing machine shops to 3D printing advantage while still keeping its original operation capabilities.

## 2. METHODOLOGY

### 2.1 Feasibility study and testing of the 3D metal printing/machining system concept

Initially, we defined parameters for a 3D metal printer with machining capability as an alternative to the more expensive options currently available This machine can deposit and remove metal material to create a workpiece. This technology follows the 3D design created using a 3D solid modeling application, crates a program, and uploads it to the 3D printer to produce functional parts. The machine can withstand higher temperatures needed to work with molted metals while maintaining the desired accuracy in machining. A set of specifications was created to keep the project on track, and a set of benchmarks tests were accomplished.



***Cite this article as:*** *Ikonomov, P. (2020). HYBRID 3D METAL PRINTING. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

Figure 1. 3D metal printing (left) and machining processes

We had investigated suitable metal 3D printing technology for metal deposition. We examined several methods for 3D metal printing to deliver material layer by layer. We found that one common way to deposit build material is gas metal arc welding (GMAW), commonly called metal inert gas (MIG) welding. It provides a sufficient method to build the material structure but lacks a building precision. Initially, we developed and built a simple prototype machine using MIG welding and machining controlled by a CNC machine. Although the testing process and the prototype machine were not fully automated completed, we successfully produce good quality samples. This proof of the concept prototype facilitated us to refine the concept to build a system to function automatically.

### 2.2 Hybrid 3D metal welding/machining process interleave method

The operation process of the 3D metal printing/machining system is as follows. At the initial stage of the process, a 3D CAD solid model is used in CAM software to create the models of the additive (metal deposition) and subtractive (CNC machining) program. The Hybrid 3D printing process start after the program is loaded in the CNC system. At first, the tool with the welding head is moved in the position and deposit a thin layer of material on the substrate plate, see Figure 1 (left). The welding head movement is controlled by the CNC machine, while the welding parameters are controlled by the GMAW welder. After a layer is completed, the welding head retracts, and the cutting tool machined the layer sides following the programmed CNC path, see Figure 1. Middle and right. This process is repeated multiple times to finish the production of a part.

During the initial testing stage, we discovered that for some basic shapes, the 3D printer worked great. Although, when producing complex shapes with overhang, hollow parts, and bridges, the molted metal tends to overflow, and the sound quality could not be effortlessly achieved. We went back to refine the concept and redesigned the initial prototype to avoid these problems.

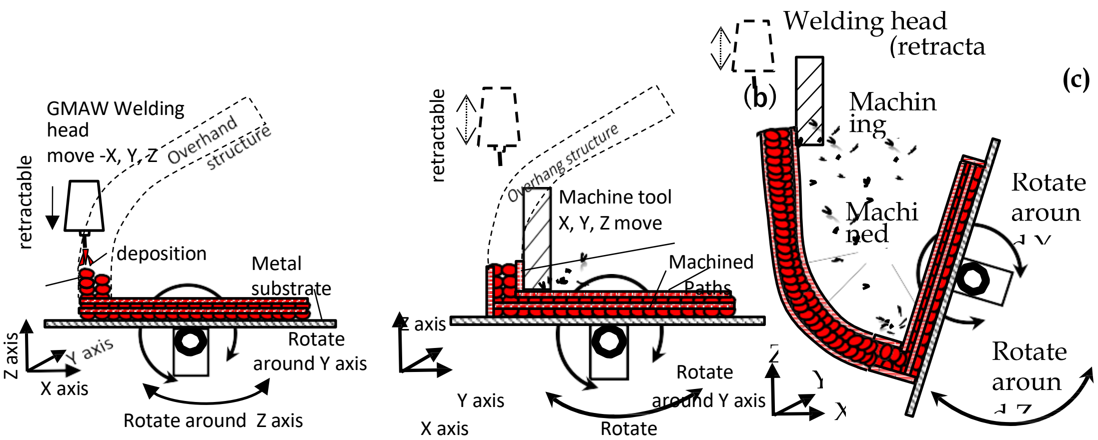


Figure 2 (a, b, c). 5 axis hybrid 3D printing-MIG welding deposition and CNC machining of overhang structure

### 2.3 The new Hybrid 3D metal printing system

A novel 3-D metal printing device and process were developed and built at Western Michigan University. This device combines GMAW welding technology (also known as MIG) with Computer Numerical Controlled (CNC) Machining. We integrate additive welding technology (the build-up of metal layers) with the subtractive/machining capabilities of CNC machines to create a unique ability for 3D component fabrication, feature addition, and repair for a wide variety of metals and metal alloys.

The machine's synchronous 5 axes, linear (3), and rotational (2) motions provide precise control of both additive delivery and machining of each layer from start to finish, see Figure2. The attached retractable welding arm is guided by the CNC controller to deposit metal precisely on a predefined path for each layer; then, the CNC machining tool removes excess material from the deposited layer. This deposition welding (additive) and machining processes (subtractive) is repeated multiple times until the final part is produced. Our hybrid system has the unique feature that it can deposit material and machine it in 5 axes, to create complex shapes, including overhang, bridges, and holes without supporting material (see Figure 2). The milling passes are capable of achieving high accuracy and surface finish on any surface in any direction without any additional setup or adjustment. Because the deposition process utilizes standard welding wire, the operating cost of our hybrid technology is relatively low, without requirements for special materials or training, resulting in a low cost per part production.

### 2.4 Hybrid 3D Metal printing prototype

We are creating a hybrid additive, and subtractive interleave process and build our first Hybrid 3D metal printing prototype from scratch. All these operations are performed on the same setup, see Figure 3.

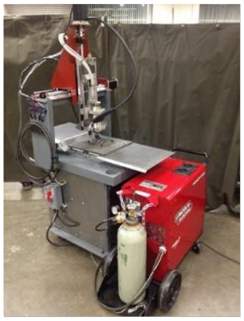


Figure 3. Hybrid 3D Metal printing prototype

The Hybrid 3D metal printing machine can produce functional parts, without using any support structure, in the one setup with high tolerance, same as CNC machining, while reduced manufacturing time and cost.

*Cite this article as:* *Ikonomov, P. (2020). HYBRID 3D METAL PRINTING. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

## 3. RESULTS AND DISCUSSION

Our hybrid technology eliminates the additional steps and costs of machining parts on separate stations, e.g., machining immediately after each layer of metal is deposited. It enables the manufacture of 3D printed parts with complex geometries (including overhangs and cavities) without using support structures–– required with existing 3-D metal printing technologies.

We are creating a hybrid additive and subtractive interleave process for our Hybrid 3D metal printing technology using CAM software to create the automation program. All these operations are performed on the same setup and without using any support structure.

### 3.1. 3D Metal printing problems and our solution

There are several problems that other 3D metal printing technology have, such as overhang/hollow structures, low-quality surface finish, and tolerance, etc. For example, existing 3D metal printers design with an overhang structure greater than 0.020 inch (0.5mm) requires additional support to prevent damage to the part [11], see Figure 4.

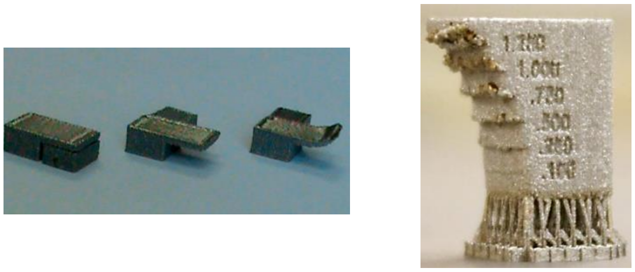


Figure 4. Existing metal 3D printing problems-overhang structures [11].

Our technology provides capabilities, in addition to three linear motions, to rotate the table to any angle to create effortless overhang structures without support that are also precisely machined, as shown in Figure

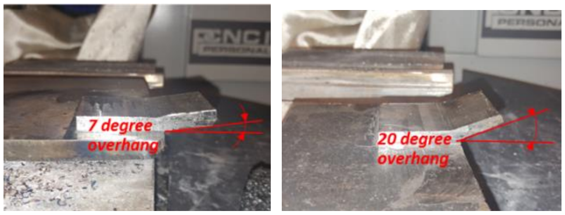


Figure 5. Hybrid technology allow 3D print and machining without any overhang.

Other problems for 3D printing are producing complex overhand structures such as bridges - flat down-facing surfaces supported by two or more features with minimum unsupported -0.080 inch (2mm) and holes (Figure 6.) and channels not exceed a diameter of 0.30 inch (8mm), [11].

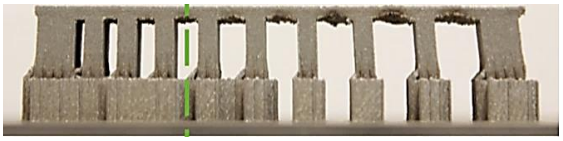


Figure 6. Existing metal 3D printing -bridges and complex structure [11]

Again our technology proved the we can build not only simple overhang structures, like single bridges or even multi-story bridges, as shown in Figure 7.

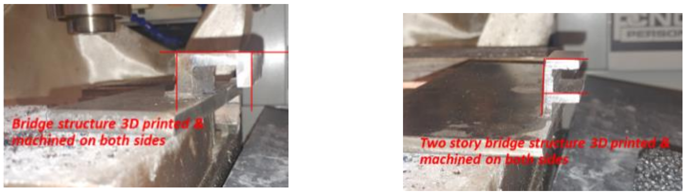

Bridge structure 3D printed &
machined on both sides
Two story bridge structure 3D printed &
machined on both sides

Figure 7. Hybrid technology allows 3D print and machining single or multistore bridges

Furthermore, we can produce parts with intricate geometry and inner surfaces normally unreachable by any CNC machining tool, see Figures 8 and 9.

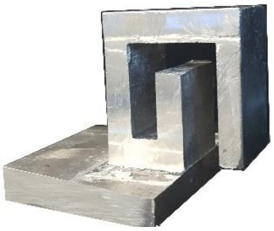


Figure 8. Hybrid 3D printing aluminum of spiral surface machined inside/outside.

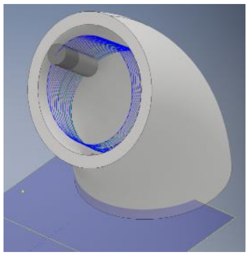


Figure 9. Hybrid 3D design of toroidal surface machined inside/outside.

In general, existing 3D metal printing technology produces inferior quality parts with relatively low tolerances for metal 3D printing features +/- 0.020 inches (0.5mm); furthermore, the printed surface finish is very low that made produced parts impossible to assemble [12]. To make parts functional, secondary machining, on separate machines and setup, are required to remove support structures and provide suitable tolerance and surface finish.

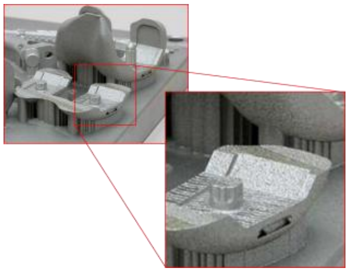


Figure 10. Existing metal 3D printing quality problems- removing support structure, tolerance, surface finish [12, 13].

Our Hybrid 3D metal printing technology provides the same quality as CNC machining with tolerances in range 0.001 to 0.0001 in and superior finish, all on the same machine and setup (Figure 11).

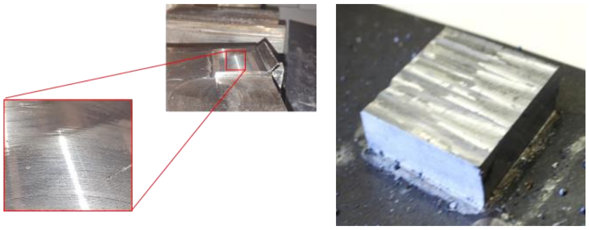


Figure 11. Hybrid 3D metal printing delivers same quality as CNC machining process

### 3.2 Hybrid 3D metal printer result and testing

We have created a hybrid additive and subtractive process for our Hybrid 3D metal printing technology using CAD/CAM software that can produce:

- **High quality finished parts:** All additive/subtractive operations are performed on the same setup with superior CNC quality.
- **Complex geometry without support material:** Our technology allows the production of finished machined parts with complex 3D geometry on the same machine, without the need for any support structure.
- **Structures with isotropic properties in any direction:** Our machine can deposit and subtract metal in any direction utilizing 3 linear axes and 2 rotational axes. We have produced samples by adding metal, layer by layer, in specific patterns: along the X-axis direction, across Y-axis, at 45°angle, and vertical Z-axis (Figure 12) and have tested the mechanical and microstructural properties using destructive and non-

destructive methods. The results show almost identical isotropic mechanical properties, metallurgical properties, and superior surface finish in all directions [14].

- **Testing process and optimization:** We proved that our Hybrid 3D metal printing technology could produce complex geometry parts with precision dimensional accuracy, meeting the design specifications.

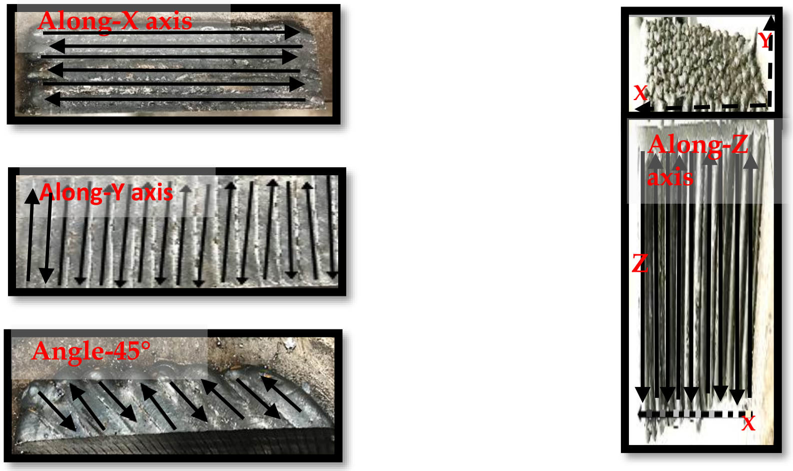


Figure 12. Hybrid 3D printing layers' directions: along X axis, across Y axis, at angle 45°, and vertical Z axis.

Furthermore, we have tested and evaluated that the Hybrid process is capable of fabricating fully dense metal parts, isotropic in all directions with mechanical properties better than bar stock material.

For example, the average yield (YTS) and ultimate (UTS) tensile strength of 3D printed tensile specimens is 395MPa and 500MPa, which are better compared to standard AISI 1018 mild/low carbon steel (YTS 370MPa & 440MPa). The Rockwell B (90-98) and Brinell hardness (170-178) numbers are also better than AISI 1018 mild/low carbon steel (HRB 71 and Brinell 126), for more details refer to results listed in our publication [14].

- **Built parts for industry:** We have made multiple complex geometry parts with a superior surface finish and tight tolerances. These sample parts are 3D printed and machined on the same setup. Most of these parts were made for industrial customers who successfully tested them inside their equipment, see Figure 13.

***Cite this article as:*** *Ikonomov, P. (2020). HYBRID 3D METAL PRINTING. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

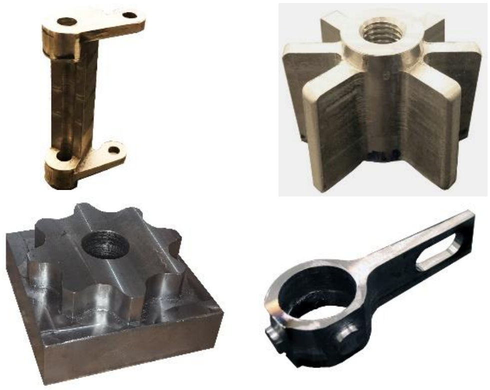


Figure 13. Sample parts produced for industrial customer.

Figure 13. Sample parts produced for industrial customer.

We had proved that the Hybrid 3D metal printing machine could produce functional parts in the same setup with high tolerance, same as CNC machining, while reduced manufacturing time and cost. This hybrid concept can be effortlessly incorporated as add on kit to new or convert existing any CNC machine to a hybrid 3D metal printer. It can produce metal parts without the need for special training for the operator while still retaining the original machining capabilities.

## 4. CONCLUSIONS

We completed and tested the functionality of the Hybrid 3D metal printing/machining prototype system. One of the best advantages of the proposed technology its capability to produce high quality finished functional parts in one setup. The advantage of using the hybrid 3D printing process and machining is that the quality of every layer is controlled precisely, thus make it possible creating of finished complex surfaces, isotropic in all directions, with intricate internal and external shapes. Such achievement cannot be accomplished with traditional CNC machines or 3D printers. In contrast to the metal powder-based technologies used by other 3D metal printers, the material used in this technology, GMAW welding wire, is broadly commercially available produced in large quantities and doesn't need special requirements for storage and operation. This Hybrid technology is significantly lower in initial cost and cost to operate. It has a small facility footprint as it constitutes nothing more than an add-on accessory to a new or an existing CNC machine.

## REFERENCES

1. Beth McKenna, 3-D Printing in the Aerospace Industry: How General Electric and United Technologies Are Using This Technology, retrieved on 10/18/ 2019, http://www.fool.com/investing/general/2014/02/28/3-d-printing-in-the-aerospace-industry-how-general.aspx

***Cite this article as:*** *Ikonomov, P. (2020). HYBRID 3D METAL PRINTING. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

2. Tomas Kellner, (2017), Mind Meld: How GE and A 3D-Printing Visionary Joined Forces, retrieved on October 18, 2019, https://www.ge.com/reports/mind-meld-ge-3d-printing-visionary-joined-forces/
3. Jessica Van Zeijderveld, State of 3D Printing 2018: The rise of metal 3D printing, DMLS, retrieved October 18, 2019, https://www.sculpteo.com/blog/2018/06/12/state-of-3d-printing-2018-the-rise-of-metal-3d-printing-dmls-and-finishes/
4. Wohlers Report, Wohlers Associates. Wohlers Report 2018: 3D Printing and Additive Manufacturing State of the Industry, Annual Worldwide Progress Report. (ISBN 978-0-9913332-3-3).
5. Anatol Locker, The metal 3D Printer Guide – All About Metal 3D Printing retrieved on October 18, 2019, https://all3dp.com/1/3d-metal-3d-printer-metal-3d-printing/
6. First titanium 3D-printed part installed into serial production aircraft, retrieved on October 18, 2019, https://www.airbus.com/newsroom/press-releases/en/2017/09/first-titanium-3d-printed-part-installed-into-serial-production-.html
7. Premiere at Mercedes-Benz Trucks: New from the 3D printer: the first spare part for trucks made of metal, retrieved on October 26, 2019, https://media.daimler.com/marsMediaSite/en/instance/ko/Premiere-at-Mercedes-Benz-Trucks-New-from-the-3D-printer-the-first-spare-part-for-trucks-made-of-metal.xhtml?oid=23666435
8. Ready for mass production: Volkswagen uses the latest 3D printing process for production, retrieved on October 26, 2019, https://www.volkswagenag.com/en/news/2018/09/volkswagen_3d_printing.html
9. Tomas Kellner, (2017), Mind Meld: How GE and A 3D-Printing Visionary Joined Forces, retrieved on January 20, 2019, https://www.ge.com/reports/mind-meld-ge-3d-printing-visionary-joined-forces/
10. US Patent US20170144242A1 (2016), Jim Mcqueen, Daniel Ziemer, Matt Ziemer, Jake Ives, Pavel Ikonomov, 3D Metal Printing Device and Process, retrieved from https://patents.google.com/patent/US20170144242A1
11. Jonathan Bissmeyer, Designing for the DMLS Process, Proto Labs, retrieved on January 23, 2019, https://www.slideshare.net/MecklerMedia/designing-for-the-dmls-process-oct2015
12. DMLS technology (n.d.), (Direct Metal Laser Sintering), examples, retrieved on January 23, 2019, https://dmlstechnology.com/dmls-examples

13. Larry Greenemeier, NASA Plans for 3-D Printing Rocket Engine Parts Could Boost Larger Manufacturing Trend, retrieved on January 23, 2019, https://www.scientificamerican.com/article/nasa-3-d-printing-sls-rocket-engine

14. Swanand Pavanaskar, Pavel Ikonomov, Prashant Gunai, David Mawma, Testing Mechanical Properties of Hybrid 3D Metal Printed Parts, RAPID 2019 conference, Detroit, May 20 - 24 2019.

15. Vikram Srinivasan, Pavel Ikonomov, Avinash Srinivas and Van Bawi Lal, Hybrid 3d Metal Printing & Process Improvement, RAPID 2019 conference, Detroit, May 20 - 24 2019.

| ISBN | 978-93-88122-13-9 |
|---|---|
| Website | www.iccotwt.com |
| Received | 26 June 2020 |
| Article ID | iccotwt.2613 |

| VOL | 01 |
|---|---|
| eMail | iccotwt@asdf.res.in |
| Accepted | 03 July 2020 |
| eAID | 2020.iccotwt.2613 |

# CHARACTERIZATION OF THE-MECHANICAL PROPERTIES OF PARTS PRODUCES WITH A HYBRID 3D METAL PRINTER

**Pavel Ikonomov[1] , Sudarshan Rawale[2]**
*Western Michigan University, Kalamazoo, Michigan, USA*

**ABSTRACT:** 3D printing, also known as Additive manufacturing and rapid prototyping in the pasts has been growing exponentially in reset years. While plastic 3D printing is widely used, 3D metal printing has limited applications due to several factors. To make functional metal parts, the technology needs to be tested and compared with existing metal fabrication technology. We will discuss testing the physical, mechanical, and metallurgical properties of the parts produced with the Hybrid 3D metal printer. Our printer uses GMAW welding and CNC machining, two widely used methods in industry-developed to a novel hybrid system that can produce a part in one setup. We did our testing following the regulation by ASTM and ISO 3D printing standards and NIST Additive Manufacturing Benchmark Test Series (AM-Bench). We used standard methods to evaluate tensile and bending strength, hardness test, micrograph with optical and microscale laser microscopes, surface rouges, CT X-ray scan, and laser and white light 3D scanning. The result proved that our technology can produce parts with mechanical properties exceeding the standard wrought metal products.

**Keywords:** Three dimensional printing, mechanical properties, hybrid metal printing, additive manufacturing, characterization.

***Cite this article as:*** *Ikonomov, P., & Rawale, S. (2020). CHARACTERIZATION OF THE MECHANICAL PROPERTIES OF PARTS PRODUCES WITH A HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

# 1. INTRODUCTION

Additive Manufacturing (AM), also called 3D printing, has been primarily focused on thermoplastic components but is rapidly growing to include metal 3D parts. Powder bed fusion, binder jetting, direct energy deposition, and material extrusion are the most common technologies employed for producing 3D metal parts. Based on the 3D printing method, metal parts are produces differ in their quality, size, cost, and mechanical properties.

## 1.1 Metal 3D printing technology

MBF: One of the 3D printing technology, metal powder bed fusion (MBF), includes three subtypes: direct metal laser sintering (DMLS), selective laser melting (SLM), and electron beam melting (EBM). SLS technology works by spreading a thin layer of powder on flat surface; the power laser/beam melt it the desired path; the process is repeated multiple times complete the part. Depends on the technique, SLS and DMLS can create parts by implementing sintering or melting. SLS is using one metal when DSLM metal alloys.

Sintering produces parts with porosity and needs a heat treatment after the print to melt and joint particle; therefore, they could not reach density and mechanical properties of the solid metal. At present most of the SLS and DMLS machines use melting. Instead of a laser, EMB employs high-power electronic beam that makes them capable of printing with high-temperature metal alloys [1].

MBF advantages pose advantages such as using various metals and alloys, mechanical properties matching wrought metal, and processing are the same as regular metal parts. Disadvantages are that parts need designed support structures and build plates, require additional secondary operations to remove excess material, prints are small sizes, and uses expensive machines, operations, and metal powder [2].

**MBT:** Another 3D printing technology, Metal Binder Jetting (MBT), uses inkjet-based process spraying binder onto the metal powder. It is based on the technology developed at MIT in '90 s, then called 3D printing [1]. MBT process starts with spreading a thin layer of powder (similar to SLS). Then the inkjet head sprays binder on the powder, and the process is repeated to create a fragile part. To produce solid parts, rebinding and sintering using a furnace are required. This method has several advantages, such as producing large parts, very fact printing, cheaper than PBF, does not need support structures and build plate.

**DED:** The third 3D printing technology, Direct Energy Deposition (DED), has two sub-types laser engineered net shaping (LENS) and direct metal deposition (DMD). DED prints by melting, with laser, electronic beam or arc, metal powder, or wire on a metal build substrate. The way it works is similar to welding [1]. The advantages of DED are large sizes, efficient material usages, fast printing, solid wrought like metal with good mechanical properties, and most unexpansive material (if a metal wire is used). Disadvantages includes: low surface quality and detail resolution, which require machining, support material is need, and uses expensive machines and operation [2].

**MME:** The fourth method is Metal Material Extrusion (MME), works similar to Fused Deposition Modeling (FDM), producing parts using plastic filament or rod with embedded metal powder. Solid parts are produced by sintering the printed parts in a furnace [3]. Advantage of this technology are that produce the most inexpensive 3D printing parts, and it is easy to operate. Disadvantages are high porosity and lower mechanical properties, require debinding and sintering, precision, and geometry restrictions related to shrinkage during sintering [2, 3].

Current 3D metal printing methods present several problems, including inconsistent material structure, uses multiple specialized chambers, uses systems expensive to purchase**,** install, operate, and maintain. Furthermore, these methods require using additional support structures which need secondary operations to remove excess material to meet tolerance requirement and surface finish. These challenges call for an innovative 3D metal printing device that is simple, inexpensive, and easy to operate.

### 1.2 Hybrid 3D Metal Printing Technology

A novel 3-D metal printing device and process were developed and built at Western Michigan University [4]. This device marries Gas Metal Arc Welding (GMAW, also known as Metal Inert Gas MIG) with Computer Numerical Controlled (CNC) Machining. It integrates additive welding technology (the build-up of metal layers) with the subtractive/machining capabilities of CNC machines. The welding arm is guided by the CNC controller to deposit metal precisely on a predefined path for each layer; then, the CNC machining tool removes unwanted material after each additive layer is deposited. This deposition welding (additive) and machining processes (subtractive) is repeated multiple times until the part is produced. This process of integrating additive with is subtractive processes enables fabrication of complex geometries (e.g., overhangs, cavities) without using support structures usually required by other AM technologies.

The innovative hybrid 3D metal printing technology fulfills the industry's needs for an economical, zero-footprint solution for the rapid fabrication of complex metal components. The hybrid 3D metal printer technology can be incorporated directly onto new or existing standard CNC mills already a part of a machine shop, with near-zero incremental footprint to the facility, and utilizes standard commercial welding wire as the raw material input.

Advantages of this approach to metallic Additive Manufacturing include lower capital cost, smallest footprint, lower operating cost, unlimited scalability, and inherently full density printed components with final form and finish directly from the machine without the need for secondary operations. Commercial applications include manufacturing plants, maintenance shops, and isolated remote fabrication/repair facilities.

## 2. METHODOLOGY

### 2.1 Why this extensive testing is needed?

To make 3D printing the next stage in the new technology there is a need to prove that this technology can meet the requirement regarding material quality. The new 3D metal printing technology poses new challenges regarding the testing of the material structure of the parts produced with our hybrid methods. Casting, welding, and machining are all well-established processes with a clear path for testing material structures and mechanical properties. The hybrid 3D metal printing process and its products, which can be considered as a combination of these three technologies, is completely new and not well investigated. Due to the intensive heating-cooling process during metal deposition, tiny defects such as pores or cracks can appear in the layers reducing mechanical properties of the part. For example, when layers are deposited over each other as they cool residual stress can accumulate creating cracks between some of the layers and even wrapping the surface. Therefore, the 3D metal printing process requires superior control to avoid defect and changes within the internal structures of the material and material properties need to be tested thoroughly.

3D printing parts, depending on the process parameters, can have anisotropic properties [5, 6]. For example, depending of the direction of deposition of material most 3D printed produce layer with isotropic properties on XY direction but the properties in Z direction are lower. These properties also depend on the deliver path directions and width, and layers thickness. For example, structure may be different for the material deliver on X-axis direction, from one drive on the crossways pattern along Y axis ($90^o$ degree to X), from one delivered at $45^o$ degree from X, and considerable different on vertical Z-axis, see Figure1.

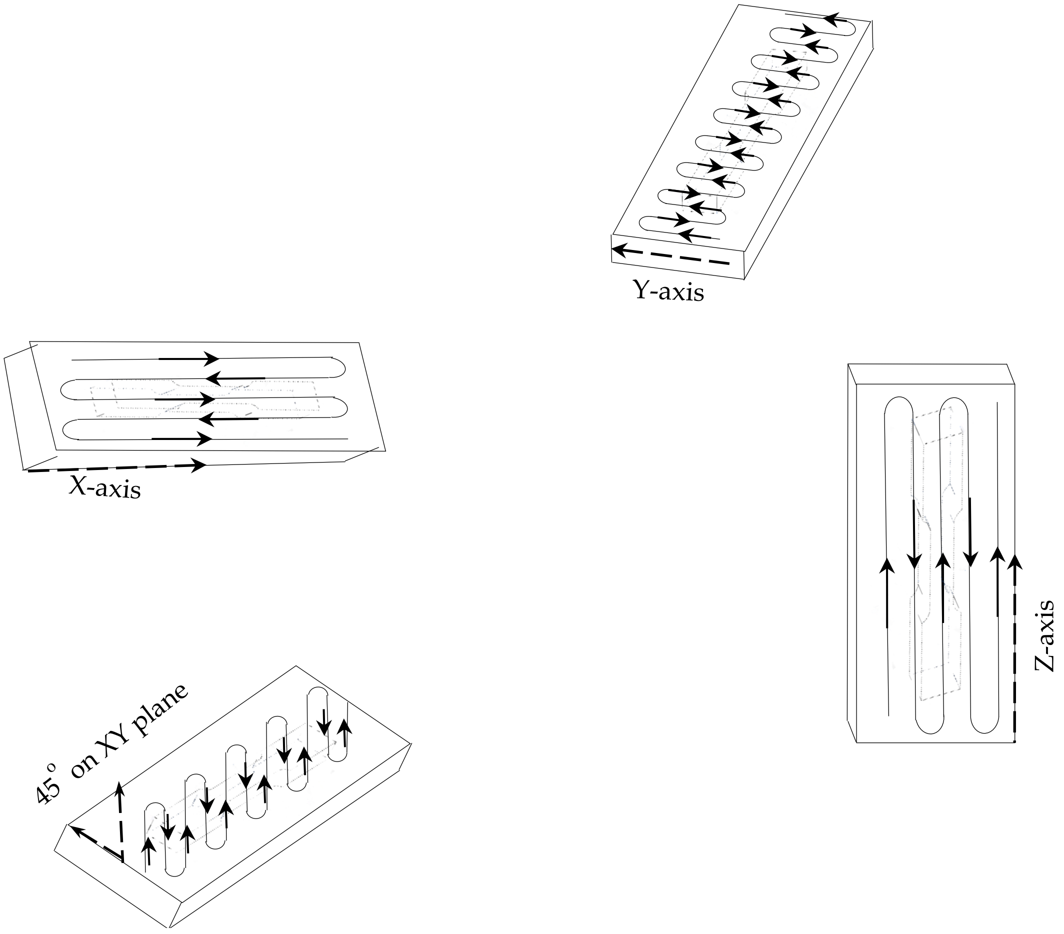


Figure 1. Deposition directions: along on X –axis, across on Y-axis, on $45^{o}$, and on vertical Z-axis

There are many government and industrial standards works in progress to make sure that 3D metal printer parts are testing to meet the industrial requirements. As discussed at ASTM and NIST a workshop May 4-5, 2016, there are metal additive manufacturing (AM) products applications where fatigue and fracture are critical [7]. NASA is well known for its pioneer efforts in AM implementation and usage while applies strict standards requirements to be met for any product used in the space industry [7, 8]. The draft NASA MSFN standard lists "four fundamentals aspects for process control of AM"… to achieve products with reliable mechanical properties: Metallurgical Process Control, Part Process Control Equipment Process Control, and Build Vendor Process Control." According to these standards, the AM produces unique material product form each single AM machine the process need to be qualified separately. Witness samples allow testing without handling the actual part, to ensure the 3D metal printing process is accurate before moving forward with the actual product. Witness specimens provide direct evidence only for the systemic health of the 3D printing process during the witnessed build [8].

To meet the requirement of the industry AM and in particular our hybrid metal 3D printing process, rigor standard requirements need to meet when building products.

### 2.2 Testing of 3D printed products

Samples produced with our hybrid 3D metal printer need to be tested to meet requirements for quality parts. Apart from dimension and tolerance requirement to be met by the production, we decide to perform the following tests [9].

#### 2.2.1 Destructive testing

**Tensile testing:** Tensile testing measures the strength of a 3D metal printed and machined sample locate midway between the jaws of the testing machine. The width thickness of the test specimen is measured before testing. The tensile strength is calculated by divide the load by the cross-section area of the middle of the sample. b. The shearing strength of transverse and longitudinal fillet welds is determined by tensile stress on the test specimens. The shearing strength of the weld in pounds per linear inch is determined by dividing the maximum load by the length of fillet weld that ruptured [10, 11].

Bend testing: It provides values for the modulus of elasticity in bending, flexural stress, flexural strain, and the flexural stress-strain response of the material. It deforms the test material at the midpoint forming a bend without fracture [10].

**Hardness testing:**_Hardness is the resistance to indentation, and it is determined by measuring the permanent depth of the indentation. The indentation hardness value is obtained by measuring the depth or the area of the indentation using a ball-shaped indenter for the Brinell hardness test or cone for the Rockwell test. Appropriate methods will be selected depending on the welding materials and heat treatment [10].

**Macro etching testing:**_The acid reacts with cracks edges and accentuates the weld defects. Small samples are polished and then etched. The cracks are inspected visually and measured for lack of fusion, porosity, cracks, and others. [10, 11].

#### 2.2.2Nondestructive testing

**Liquid penetrant testing:**_Liquid penetrant testing is also called dye penetrant inspection. It is one of the most commonly used crack detection methods for of surface-breaking discontinuities. It can reveal discontinuities problems or pores internal to the weld. There are two methods, using the so-called visible die or fluorescent dye. With the visible die, a colored die is used with a white developer to increase the contrast and make it visible under regular light. Similarly, when the fluorescent dye is applied, then the developed is applied later to increase penetration to the surface imperfection. Then a black light is used to the high contrast between the fluorescent material and sample reveal the defects [12, 13].

**Magnetic particle testing:** It is used to detect cracks, porosity, seams, and inclusions, lack of fusion, surface discontinuities, and shallow subsurface discontinuities in ferromagnetic materials. When applying a magnetic field to a part, it attracts the magnetic particles to the crack or imperfection places [10, 12].

**CT X-Ray testing:** This is a radiographic test method used to reveal the presence and nature of internal defects in a weld, such as cracks, slag, blowholes, and zones where proper fusion is lacking. Gamma provides deeper penetration allowing thicker walls to be inspected but is slower [12-13].

### 2.2.3 Metallurgical testing

Although the metallurgical tested will be performed during the project, the information for grain size, expected phases or carbide sizes, grain boundary cleanliness, porosity, lack of fusion/cracks were used to correlate these result with the one investigated by this research.

## 3. RESULTS AND DISCUSSION

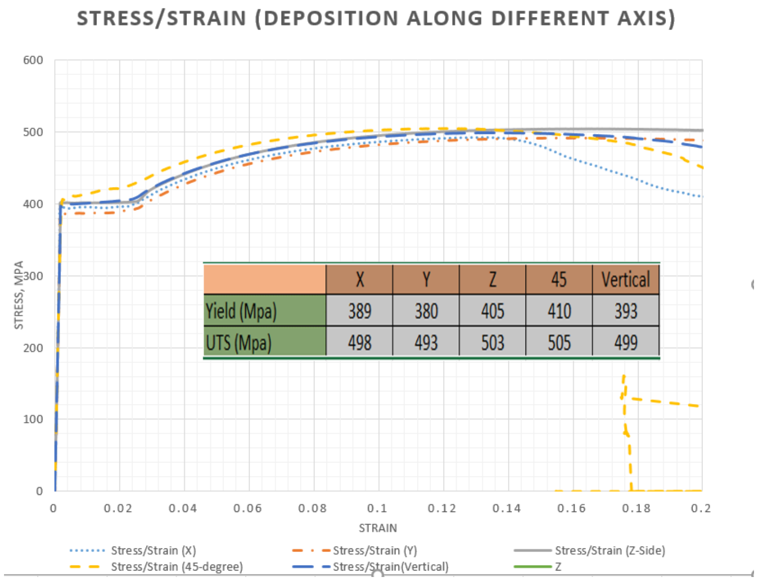
### 3.1 Destructive testing

During the technology development and testing, we have optimized the 3D printing and CNC machining, so our final results show no cracks porosity and imperfection on any samples. They were produced with different directions of the 3D printing welding delivery: along the X-axis, across on Y axis, under 45 degrees, along the Z-axis sideways, and vertical along the Z-axis. The testing proved that our technology provides the same mechanical properties (isotropy properties of the material) in all directions.

**Tensile testing:** The test samples were prepared as per ASTM E8/E8M-16a standards [14]. Sub-sized specimens were used, with dimensions of 100x6x6 mm (LxWxH). Twenty-five samples we created for each direction, X, Y, Z, 45o degree, and vertical side, of materials delivery. The shield gas ratios used were Argon30%/$C0_2$70%. After each layer was delivered, the top for the layer was machined to produce a smooth surface for the next layer. This process assured the quality of the welding and the constant height of the delivery pattern.

We tested more than 125 tensile samples using disposition the specified above five different directions of the welding material deposition. According to the results, the average yield & ultimate tensile strength for all the direction of deposition is 395 MPa and 500MPa, respectively, see Figure 2.

According to ER70S-6 Gas Metal Arc Welding (GMAW) wire technical specification sheet, ultimate strength, and yield strength are 586 MPa and 483 MPa respectively [15. In addition to wire material properties, we compared our 3D printed test results with ASTM A36 Mild/Low Carbon Steel [16], which has the yield and ultimate tensile strength between 380 MPa and 505 MPa respectively. The result shows that our 3D printed samples have the same or better tensile properties when compared with GMAW welding wire MDS specifications and higher than ASTM A36 Mild/Low Carbon Steel. The test also confirms the isotropic mechanical properties of the parts produced with this technology. There was not much difference in the tensile properties when metal was a deposit in a different direction.



| | X | Y | Z | 45 | Vertical |
|---|---|---|---|---|---|
| Yield (Mpa) | 389 | 380 | 405 | 410 | 393 |
| UTS (Mpa) | 498 | 493 | 503 | 505 | 499 |

Figure 2. Tensile testing X, Y, Z, 45 degrees and side directions of material delivery

**Bend tests:** It provides values for the modulus of elasticity in bending, flexural stress, flexural strain, and the flexural stress-strain response of the material. Our 3D printed samples have identical or better bending properties when compared with ASTM A36 Mild/Low Carbon Steel.

**Hardness testing:** Our 3D printed samples (Average Brinell 173, Hardeners Rockwell B 94.8, Hardeners Rockwell C 65, have identical or better hardness properties compared with GMAW welding wire MDS specifications and higher than ASTM A36 Mild/Low Carbon Steel [10, 16, 17].

### 3.2 Nondestructive testing

**Liquid penetrant testing:** Liquid penetrant testing, also called dye penetrant inspection, is one of the most commonly used crack detection methods for of surface-breaking discontinuities [17, 18]. We applied for liquid penetrant Cantesco D101-A dye penetrant developer, and Cantesco P301W-A white visible dye penetrant. We found that the common deposition approach, when welding layers were deposit directly on the previous deposit one, the 3D metal printer may produce cracks or pores between layers, mostly due to incomplete overlapping of the weld bids or imperfect weld penetration. Therefore, we designed the hybrid 3D printing process that includes machining of each layer before the deposition of the new layer we did not observe any cracks or pores.

### 3.3 Metallurgical testing

The metallurgical microstructure was performed to check the grain boundary cleanliness, porosity, lack of fusion/cracks to prove the process quality of our hybrid technology [19]. Samples we cut in three planes XY, YZ, XZ for each of printing X, Y, Z, 45° direction.

First, the microstructure testing was performed using Nikon optical microscope with x400, x1,000, and x1,500 magnifications, and no porosity, cracks, and other imperfection were found.

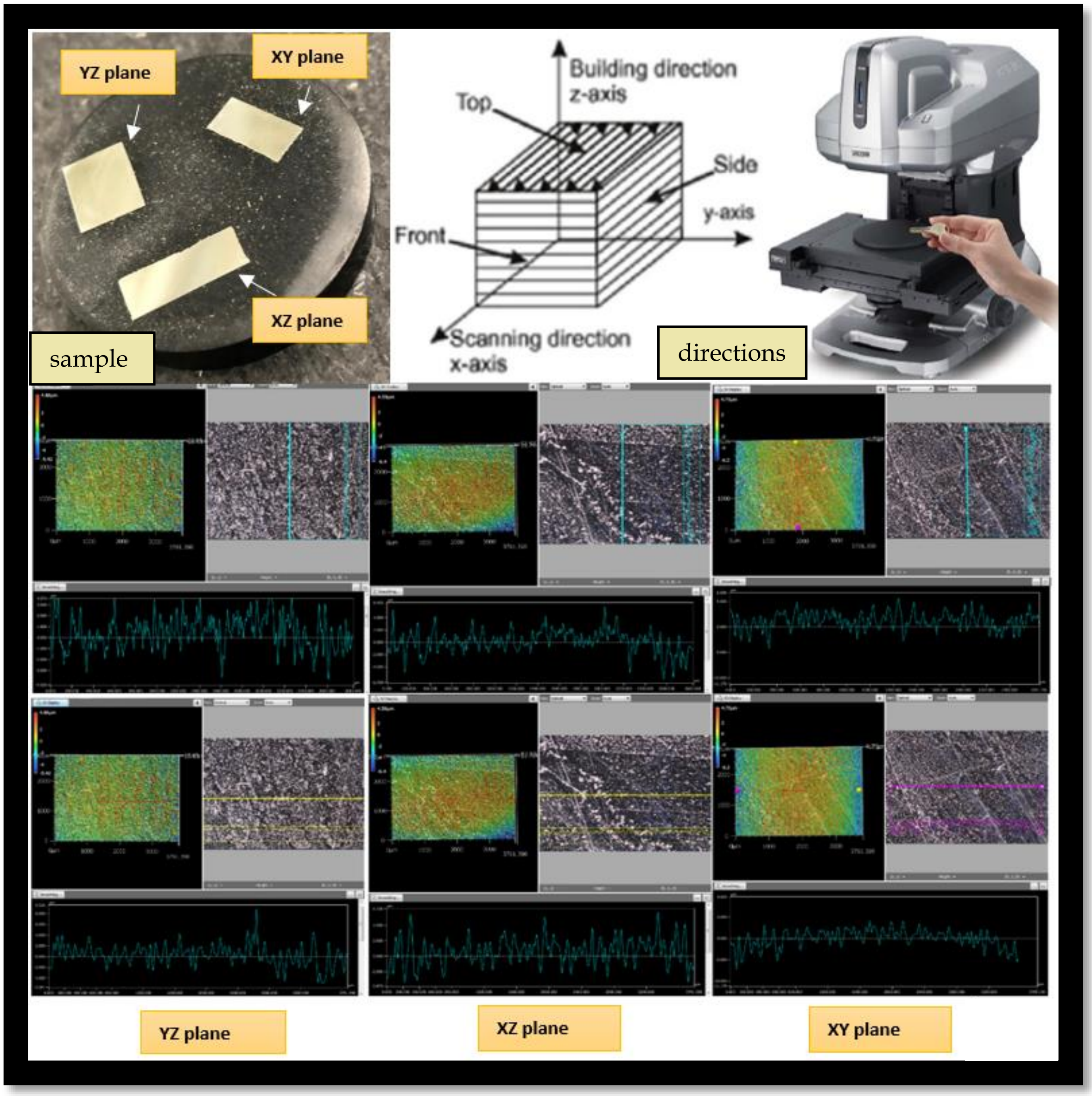


Figure 3. 3D surface finish and deviations in micrometers

Also, Keynce MicroscopeVR-3000 with resolution 1 µm was used to measure 3D surface imperfection of the samples. Roughness, flatness, form, contour deviations, and 3D analysis functions, such as height differences, area, volume, and roughness, were performed. Again not pores and cracks were found on any sample. The roughness from the 3D metal printing and machining is the same as after a standard CNC milling process. Depending on the cutting speed and federate, the average measure Ra values were 0.57 µm (between 16 and 32 µin.), see Figure 3.

**CT X-ray scans:** CT X-ray scans were performed on several parts before delivering them to the user. No imperfection such as crack, cavity, and porosity was observed, see Figure 4 for details.

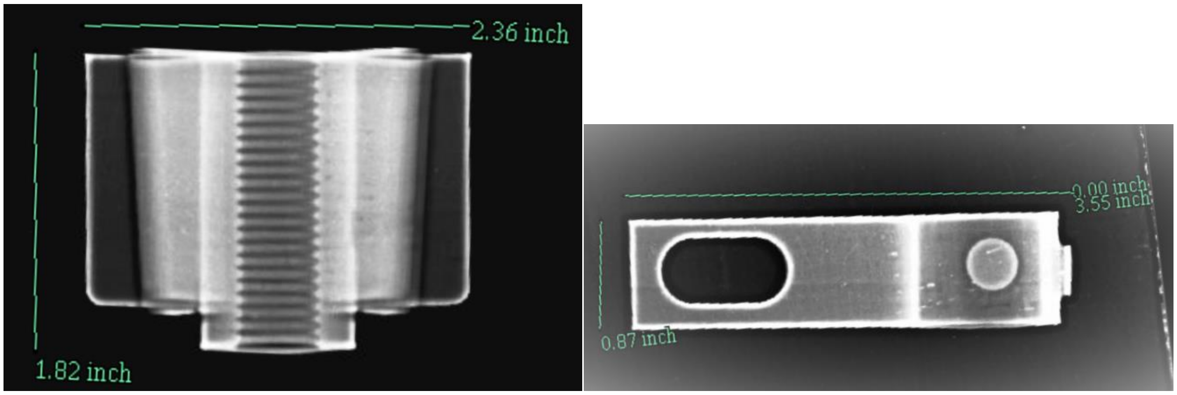


Figure 4. CT X-ray scans of parts #2 and #1 produced for a company

Finally, a new digital Keynce Microscope VHX-7000 series with magnification up to 6000 times and resolution 0.5 microns was used to measure 3D printed surface. No cracks, pores, cavity are observed on any measured surface. The only visible imperfections noticed were few microns elevated surface bumps left from the tool marks after machining the surface of the sample.

The overall testing results proved that the hybrid technology we developed could produce parts with isotropic mechanical properties, superior internal/external structures, and surface finish.

## 4. CONCLUSION

We have developed and tested the performance of our novel hybrid Hybrid 3D metal printer system that can produce quality parts in one setup. Testing was performed following the requirements of existing ASTM and ISO standards for 3D printing and the NIST Additive Manufacturing Benchmark Test

Series (AM-Bench). We optimized our process to produce multiple samples in multiple delivery directions (X, Y, Z, 45o) to teste the mechanical and metallurgical properties. We evaluated properties using tensile and bending strength, hardness test, micrograph structures with optical and microscale laser microscopes,

***Cite this article as:*** *Ikonomov, P., & Rawale, S. (2020). CHARACTERIZATION OF THE MECHANICAL PROPERTIES OF PARTS PRODUCES WITH A HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-12). London, GB: ASDF International.*

surface roughness, CT X-ray scanning, laser, and white light 3D scanning. The result proved that our technology could produce parts with superior isotropic mechanical properties exceeding the standard wrought metal products.

We have produced multiple parts for several companies that are successfully using. The results from the testing and real applications prove that our hybrid 3D metal printing technology is ready for industrial application.

Future work to be done includes optimization of the Hybrid 3D metal printing process, adding sensor based closed-loop feedback capabilities, and testing other all available GMAW wieldable materials.

## REFERENCES

1. Wohlers Report 2018, Annual Worldwide Progress Report, 2018.
2. Metal 3D Printing: An Overview of the Most Common Types, retrieved on 06/12/2020, https://3dprinting.com/metal/types-of-metal-3d-printing/]
3. Timothy W. Simpson TIMOTHY W. SIMPSON, Material Extrusion: Now with Metal, retrieved on 06/12/2020, https://www.additivemanufacturing.media/blog/post/material-extrusion-now-with-metal
4. US Patent US20170144242A1 (2016), Jim Mcqueen, Daniel Ziemer, Matt Ziemer, Jake Ives, Pavel Ikonomov, 3D Metal Printing Device and Process, retrieved from https://patents.google.com/patent/US20170144242A1
5. Chee Kai Chua, Chee How Wong, Wai Yee Yeong, Standards, Quality Control, and Measurement Sciences in 3D Printing and Additive Manufacturing, ISBN: 978-0-12-813489-4, 2017 Elsevier Ltd.
6. Additive Manufacturing Technology Standards, retrieved on 06/14/2020, https://www.astm.org/Standards/additive-manufacturing-technology-standards.html
7. Aaron M. Forster, Materials Testing Standards for Additive Manufacturing of Polymer Materials: State of the Art and Standards Applicability, retrieved on 06/15/2020, https://www.nist.gov/publications/materials-testing-standards-additive-manufacturing-polymer-materials-state-art-and
8. Nikolas Hrabe, Nicholas Barbosa, Steve Daniewicz, Nima Shamsaei, Findings from the NIST/ASTM Workshop on Mechanical Behavior of Additive Manufacturing Components, May 4-5, 2016, https://doi.org/10.6028/NIST.AMS.100-4
9. Matthews, Clifford (2001), ASME engineer's data book, ASME Press, p. 211, ISBN 978-0-7918-0155-0.
10. Welding test, retrieved on January 9, 2018, http://www.angelfire.com/my/welding/test.html
11. Esab, Introduction to destructive weld testing, retrieved on January 9, 2019, n**http://www.esabna.com/us/en/education/blog/destructive-testing-of-welds.cfm**

12. Lincoln Electric, Nondestructive Weld Examination, retrieved on January 9, 2019, http://www.lincolnelectric.com/en-us/support/process-and-theory/Pages/nondestructivie-weld-detail.aspx
13. Esab, Radiographic and Ultrasonic Testing of Welds , retrieved on January 9, 2019, **http://www.esabna.com/us/en/education/blog/radiographic-and-ultrasonic-testing-of-welds.cfm**
14. ASTM, I. "ASTM E8/E8M-16a: Standard Test Methods for Tension Testing of Metallic Materials." *West Conshohocken, PA, USA: ASTM International (2016).*
15. Technical Specification Sheet ER70S-6 Carbon Steel Welding Wire, retrieved on retrieved on 06/14/2020, www.unibraze.com/DataSheets/Data70S-6.pdf
16. ASTM A36 Mild/Low Carbon Steel, https://www.azom.com/article.aspx?ArticleID=6117.
17. Raj, Baldev; Jayakumar, T.; Thavasimuthu, M. (2002), Practical non-destructive testing (2nd ed.), Woodhead Publishing, ISBN 978-1-85573-600-9
18. Linkoln Electric, Nondestructive Weld Examination, retrieved on 06/15/2020, http://www.lincolnelectric.com/en-us/support/process-and-theory/Pages/nondestructivie-weld-detail.aspx
19. Moreno, Preto (2013), Welding Defects (1st ed.), Aracne, ISBN 978-88-548-5854-1.
20. Image Dimension Measurement System IM-7000 series, retrieved on 06/15/2020, *https://www.keyence.com/products/measure-sys/image-measure/im-7000/models/*

|  |  |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 24 June 2020 |
| Article ID | iccotwt.2614 |

|  |  |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 01 July 2020 |
| eAID | 2020.iccotwt.2614 |

# OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER

**Sudarshan Rawale[1], Pavel Ikonomov[2]**

[1,2]*Department of Engineering Design, Manufacturing and Management Systems,*

*Western Michigan University, Kalamazoo, MI, USA*

**ABSTRACT:** Hybrid 3D Metal Printer uses repetitive and alternate cycles of additive and subtractive processes. The additive process is Gas Metal Arc Welding (GMAW) and the subtractive process makes use of Computer Numerical Controlled (CNC) machining. To manufacture parts having zero geometrical defects, it is important to optimize these processes. This research is focused on design of experiments to find out the factors which influence the additive process in Hybrid 3D metal printing. The additive process (welding) in 3D metal printing has a major influence on the mechanical properties of the final product as during this stage the microstructure is formed. The welding parameters such as voltage, current, wire-feed rate, gas flow rate, arc stability, height and welding speed play a critical role. Porosity and hardness of the weld impacts its strength. But when the whole part is manufactured using a 3D printing process - alternate welding (additive) and milling/machining (subtractive) processes, it is important to understand how these parameters affect the microstructure and in turn, the mechanical properties of manufactured parts. Whereas all these parameters influence the outcome of the welding process, this paper only discusses the most influential factors such as wire feed speed (WFS - in/min), machine feed rate (MF - in/min) and the Trim (Arc Length Control). After optimizing the process, it also imports to check for the mechanical properties of the parts, hence various mechanical testing of printed parts using optimized process are discussed in brief.

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

**Key Words:** GMAW, hybrid 3D metal printing, MIG welding, additive process, metal 3D printing, feedback system

## 1. INTRODUCTION

Conventional 3D metal printers make use of technologies implementing either expensive or time-consuming processes or sometimes both. The products obtained from these processes still need some work to turn them into finished products. These technologies are complicated and require a lot of practice to master. Few of these technologies can be Powder Based Fusion (PBF), in which thermal energy fuses the selective regions of a powder bed to form a part/product. Selective Laser Sintering or Selective Laser Melting (SLS/SLM), Electron Beam Melting (EBM) and Direct Metal Laser Sintering (DMLS) are mainly used in the Powder Based Fusion Processes [1]. In addition to the cost ineffectiveness and the long lead-time, there are many more disadvantages that come along with these disadvantages. These parts have residual stresses which need to be relieved. Most important is that the parts manufactured are not homogenous. They develop pores which tend to be stress concentration areas and develop cracks with time. To obtain a good surface finish, these parts need a separate set of finishing processes which can be less expensive but are time consuming [1]. Also, these parts cannot be used for applications requiring high degrees of hardness.

The Hybrid 3D Metal Printer overcomes all these disadvantages while keeping the manufacturing cost, lead time as low as possible. Also, unlike the Powder Based Fusion processes, in Hybrid 3D Metal Printing, different welding wire materials can be carefully selected and used to obtain different combinations of mechanical properties of the parts. Table 1 lists welding wire material and their properties and applications that can be a basis of material selection for printing metal parts.

Table 1 List of welding materials, their AWS class and applications [2]

| | AWS Class | Applications |
|---|---|---|
| SuperArc® G4Si1 | ER70S-6 | Automotive components, automotive repair, robotic or hard automation |
| SuperArc® L-50® | ER70S-3 | Clean to light mill scale base material, sheet metal to 380-485 MPa yield strength material, Pressure vessels |
| SuperArc® L-52 | ER70S-2 | Root, fill and cap pass welding for piping industries, metal fabrication, power generation |
| SuperArc® L-56 N | ER70S-6 | Nuclear power plant construction and maintenance, robotic or hard automation, structural steel |
| SuperArc® L-59® | ER70S-6 | Automotive, pipeline & offshore, pressure vessels, heavy fabrication |

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

SuperArc® wires, manufactured by *Lincoln Electric,* is a low alloy and premium copper-coated mild steel MIG wire designed to provide consistency, feedability and arc performance. All SuperArc® wires show less spatter and extend the life of contact tip as they are surface treated with Microguard® Ultra™ [2]. The whole MIG wire product range manufactured by *Lincoln Electric* contain proper ratio of Chromium, Molybdenum, Vanadium, etc. based on the application requirements [2]. Furthermore, aluminum parts can also be manufactured using the Hybrid 3D Metal Printer. Different MIG wires with different compositions can be used in the Hybrid 3D Metal Printer while manufacturing parts that have specific application requirements. This changeability of the MIG wire, unlike other 3D metal printing technologies, makes the Hybrid 3D Metal Printer a versatile machine and gives it it's flexibility of choosing the metal composition of the manufactured parts as per the requirements.

## 2. METHODOLOGY

3D printing is a developing technology. Using polymers as a raw material to obtain a 3D part is conventional. The Hybrid 3D Metal Printer takes a leap further. The technology that is being developed at Western Michigan University's Department of Engineering Design, Manufacturing and Management is a critical combination of welding and milling machines. Welding, MIG in this case, is used as an additive process and milling/machining is a subtractive process used after each layer of the additive process. A given part, from scratch till a finished product, is a series of additive and subtractive processes. The one of the major advantages of Hybrid 3D Metal Printer, being developed at the Western Michigan University, is that machining is an integrated part of the printing process, hence the part manufactured has a good surface finish and does not need any processes like grinding, honing, chipping, etc.

### 2.1 Hybrid 3D metal printing technology

The methodology for manufacturing 3D printed metals parts is to integrate a feedback system with the Hybrid 3D Metal Printer to optimize the overall process by improving the additive process. Optimizing the additive process is a critical task as the quality of weld beads depend on multiple crucial factors such are Voltage, Current, Wire Fees Speed, Machine Feed Rate, Trim, arc stability, height, etc. Welding machines these days have a control over the voltage and current and manipulate these factors during the initial arc formation to melt the metals. But the other variable such as wire feed speed, machine feed rate and trim, height depend on the geometry of the parts being manufactured and they need to be controlled in real time. It is impractical and time consuming to interfere with the CNC program to adjust these parameters for every cycle of the additive process, depending on the geometrical constraints of the parts. One of the best ways to optimize this process is to add a feedback system in the control loop.

### 2.2 Feedback System

Each part is design with different geometrical constraints and tolerances that requires modifications during the 3D building process. Even after carefully choosing wire feed speed, machine feed rate and trim can cause the weld bead to be of poor quality at few spots and few regions of the part. Hence, to keep a check on the weld bead quality throughout the process, we need a real time feedback system. Feedback systems and controls are used widely in automated systems and machines. When we think of a next generation of our Hybrid 3D metal printer, we are developing a feedback controls system that can overcome any rework, reduce waste and the lead-time for production. At present, research is being done to integrate the Hybrid 3D Metal Printer with such a feedback controls system.

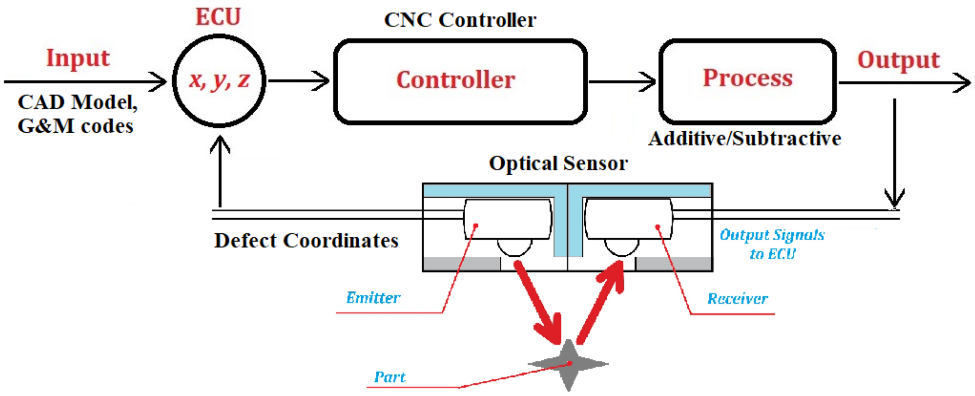


Figure 1 – Feedback System Block Diagram

The anticipated feedback module will work as shown in the block diagram in Figure 1. Once the printing process starts, a feedback sensor like a high-definition camera or a laser beam, will scan the part for irregularities, cracks, pores or contingencies and send a feedback signal to the Electronic Control Unit (ECU). The Electronic Control Unit is a computer and acts as the brain of the feedback system. The Electronic Control Unit can vary the wire feed speed, machine feed rate, height, trim and all the other parameters that can be controlled from a CNC program. The optical sensor to be used will scan the part from time to time and will compare the part with the CAD model and check for discrepancies. If the sensor senses any deflections from the required quality or dimensions of the part, the coordinates of the defect are then sent to the ECU. As the ECU is integrated into the CNC machine, it then takes over the printing process for the next additive or subtractive process cycle in order to fix the defects. The ECU also decides the process to be performed, additive or subtractive. For example, if the sensor found that there is a pore created during the last additive cycle, the ECU will send signals including the coordinates of the defect location to the CNC machine to actuate the welding process and fill the pore at the given coordinates. A similar cycle will initiate the subtractive process if there is a defect that needs subtractive cycle to fix it, for example a run down. The feedback system not only can add another additive or subtractive cycle but also can skip a cycle if the scan shows that the dimensions and quality of the part at a given point is in given tolerance. This will not only help us adhere to the quality of the finished product, but also save us time required for rework. The geometric dimensions and tolerances are important but so are the mechanical properties. Different parts can have different mechanical properties and surface finish based on their applications, for example – a gear should be hard enough not to wear out too early before its life cycle. Not only the hardness but also the porosity plays a critical role when it comes to torque or load transferring mechanical parts. Hence it is important to know how the additive parameters of the metal printing process affect the overall mechanical properties of a finished product and to form a basis to our feedback system for optimizing the additive process, we will perform a Design of Experiments. The following part of this study is focused on finding the significant parameters for the additive process as most of the mechanical properties are based on the microstructure of the material which is formed during this stage.

## 3. RESULTS AND DISCUSSION

### 3.1 Design of Experiments for Additive Process

Before developing optimization process with feedback system, it is important to investigate the 3D printing process to study and understand the factors that can be used to control the output of the process. There is a cause-and-effect relationship between the input and output of the process and to understand this relationship we must deliberately interfere with the influencing factors under study and check the effect on the output [3, 10]. For this purpose, we define an experiment with a series of runs while controlling and changing these influencing factors and understand their effect. Design of Experiments (DOE) is a tool used in the development and optimization of systems, processes and product design [3]. In this study we are performing Design of Experiments to optimize the additive process in 3D printing. The objective is to have a consistent bead size throughout the process without any pores, cavities and voids irrespective of the geometry of the manufactured part. Figure 2. shows a general model of our process [9].

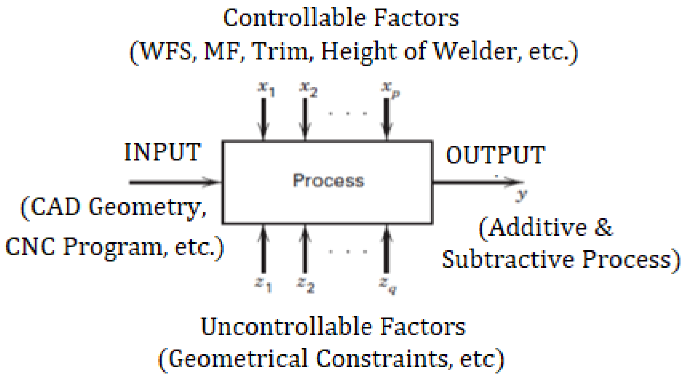


Figure 2. General Process Model [3]

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

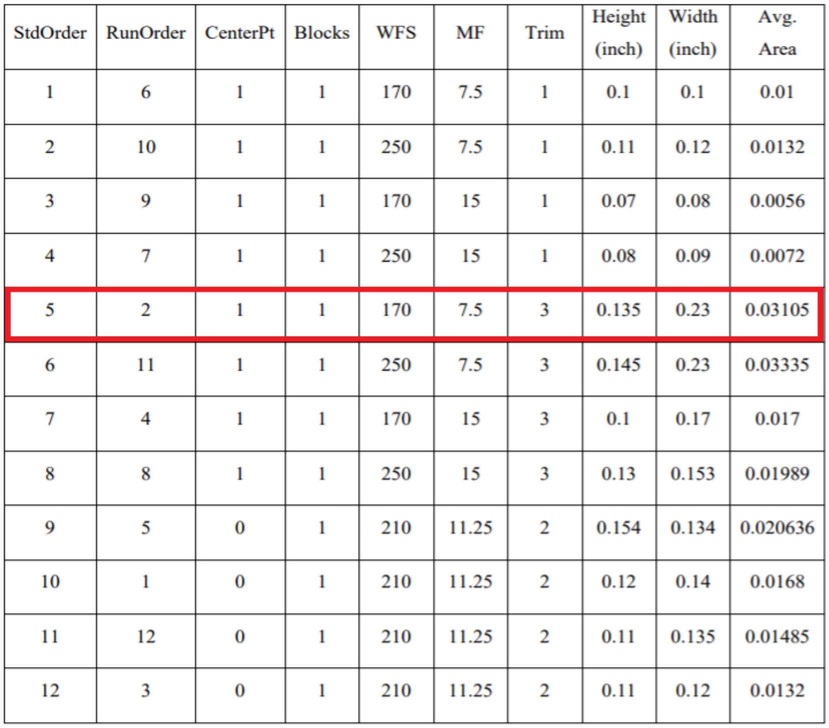
As stated earlier, the DOE was performed to optimize the additive incorporates three factors: the wire feed speed, the machine feed rate and the trim (arc length control). It is important to define the upper and lower limits for all these three factors. Table 2 lists the upper and lower limits. Using Minitab, a $2^3$ full factorial design was generated for our experiments.

Table 2 – Upper limit and lower limit of factors [9].

| Limit | Wire feed speed | Machine feed rate | Trim |
|---|---|---|---|
| Upper Limit (+1) | 250 | 15 | 3 |
| Lower Limit (-1) | 170 | 7.5 | 1 |

After noting the lower and upper limits, four center points necessary for the half normal plot were added. This helps us understand how far the factors are moving away from their mean position, eventually helping us to evaluate the most influential ones [9]. Once the most influential factors are noted, they can be optimized. Table 3 was generated using Minitab to sequence the experiment according to run order. Based on the Table 3 experiments are performed and readings for width and height of the weld bead were taken.

Table 3 – Design of Experiments with 3 factors and 4 center points [9]



| StdOrder | RunOrder | CenterPt | Blocks | WFS | MF | Trim | Height (inch) | Width (inch) | Avg. Area |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 6 | 1 | 1 | 170 | 7.5 | 1 | 0.1 | 0.1 | 0.01 |
| 2 | 10 | 1 | 1 | 250 | 7.5 | 1 | 0.11 | 0.12 | 0.0132 |
| 3 | 9 | 1 | 1 | 170 | 15 | 1 | 0.07 | 0.08 | 0.0056 |
| 4 | 7 | 1 | 1 | 250 | 15 | 1 | 0.08 | 0.09 | 0.0072 |
| 5 | 2 | 1 | 1 | 170 | 7.5 | 3 | 0.135 | 0.23 | 0.03105 |
| 6 | 11 | 1 | 1 | 250 | 7.5 | 3 | 0.145 | 0.23 | 0.03335 |
| 7 | 4 | 1 | 1 | 170 | 15 | 3 | 0.1 | 0.17 | 0.017 |
| 8 | 8 | 1 | 1 | 250 | 15 | 3 | 0.13 | 0.153 | 0.01989 |
| 9 | 5 | 0 | 1 | 210 | 11.25 | 2 | 0.154 | 0.134 | 0.020636 |
| 10 | 1 | 0 | 1 | 210 | 11.25 | 2 | 0.12 | 0.14 | 0.0168 |
| 11 | 12 | 0 | 1 | 210 | 11.25 | 2 | 0.11 | 0.135 | 0.01485 |
| 12 | 3 | 0 | 1 | 210 | 11.25 | 2 | 0.11 | 0.12 | 0.0132 |

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

Figure 3. Shows the weld beads obtained by varying these factors. The weld beads in the figure are in the standard order. It can clearly be seen from Figure 3, that the weld bead resulting from experiment 5 (standard order) was of the best quality proving that it was an optimized combination of wire feed speed, machine feed rate and trim. The same experiment 5 is highlighted in Table 3.

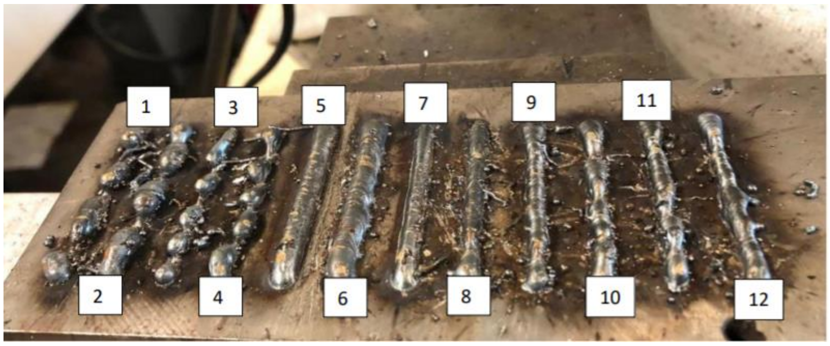
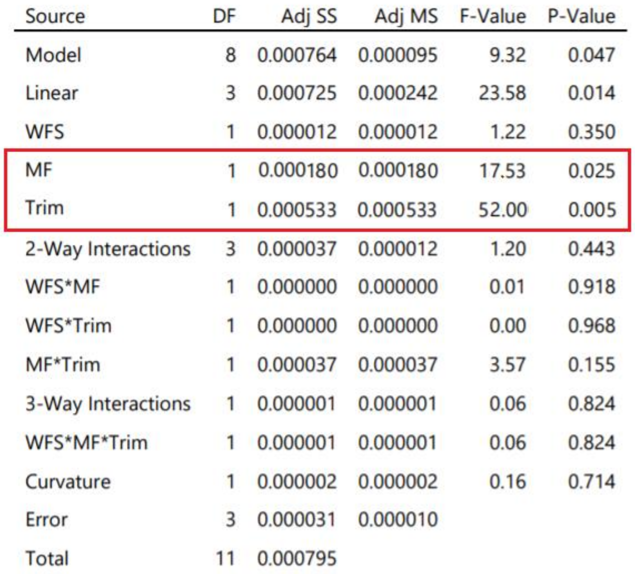


Figure 3. Design of Experiments – Weld Bead [9]

### 3.2 Analysis of Variance *(ANOVA)*

To test the equality of several means, Analysis of Variance or ANOVA is used [3]. The results from Table 3 were again used in Minitab for further evaluation. A full $2^3$ factorial design was analyzed including the four center points in Minitab to get the Analysis of Variance with a regression equation and graphical representation of half-normal plots and Pareto charts [9]. Table 4 lists the results generated after the analysis done in Minitab.

Table 4 Analysis of Variance (ANOVA) [9]



| Source | DF | Adj SS | Adj MS | F-Value | P-Value |
|---|---|---|---|---|---|
| Model | 8 | 0.000764 | 0.000095 | 9.32 | 0.047 |
| Linear | 3 | 0.000725 | 0.000242 | 23.58 | 0.014 |
| WFS | 1 | 0.000012 | 0.000012 | 1.22 | 0.350 |
| MF | 1 | 0.000180 | 0.000180 | 17.53 | 0.025 |
| Trim | 1 | 0.000533 | 0.000533 | 52.00 | 0.005 |
| 2-Way Interactions | 3 | 0.000037 | 0.000012 | 1.20 | 0.443 |
| WFS*MF | 1 | 0.000000 | 0.000000 | 0.01 | 0.918 |
| WFS*Trim | 1 | 0.000000 | 0.000000 | 0.00 | 0.968 |
| MF*Trim | 1 | 0.000037 | 0.000037 | 3.57 | 0.155 |
| 3-Way Interactions | 1 | 0.000001 | 0.000001 | 0.06 | 0.824 |
| WFS*MF*Trim | 1 | 0.000001 | 0.000001 | 0.06 | 0.824 |
| Curvature | 1 | 0.000002 | 0.000002 | 0.16 | 0.714 |
| Error | 3 | 0.000031 | 0.000010 | | |
| Total | 11 | 0.000795 | | | |

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

It is evident from the Table 4, that the *p*-value is less than the *a*-value. The *a*-value is the probability of rejecting the null hypothesis and its significant level is 0.05. It can also be seen that the *p*-value of trim and machine feed rate is less than the a-value [9]. The trim has the lowest *p*-value which suggests that the trim is one of the significant factors affecting the bead size and quality.

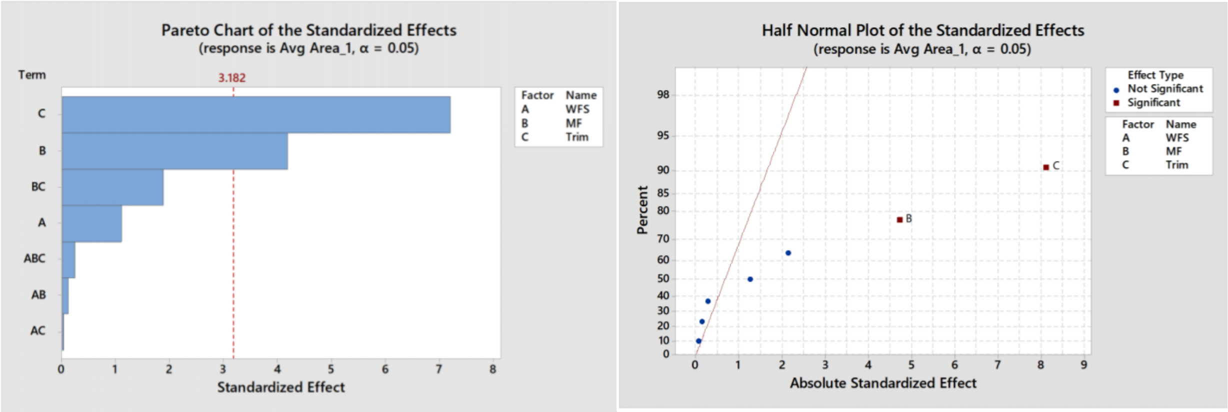


Figure 3 (a) Pareto chart (b) Half-Normal plot of absolute standardized effect [9]

From the Pareto and Half-Normal plot, it can be observed that the trim is the most influential factor of all the three factors we selected for our study, see Figure 4. The second most influential factor is the machine feed rate. From a different set of experiments, it was observed that when the machine feed rate was 8 in/min, wire feed speed of 250 in/min and a trim of 2.8, the resulting height and width of bead was 0.2 inches. Hence, it is important to optimize these factors in order to optimize the additive process [9].

### 3.3. Testing mechanical properties

For tensile testing or tension testing, samples manufactured using the Hybrid 3D Metal Printer were subjected to a monatomic tension in the axial direction. The testing samples were prepared as per the standards of ASTM E8/E8M-16a [4]. The dimensions of the specimens were 6mm x 6mm x 100mm. The testing machine used for this destructive testing was MTS 810. The behavior of the specimens was observed and mechanical properties such as Young's modulus, Poisson's ratio, percentage elongation, ultimate tensile strength and yield strength were determined.

Table 5 lists some of the important findings from the tensile testing of the printed specimens. According to the test findings, the average yield strength for the specimens for all directions of depositions is 395.4 MPa. Similarly, the average ultimate tensile strength for all directions of depositions is found to be 499.6 MPa.

**Cite this article as:**Rawale, S., & Ikonomov, P. (2020). OPTIMIZING ADDITIVE PARAMETERS AND TESTING OF THE HYBRID 3D METAL PRINTER. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.

Table 5 – Yield strength and ultimate tensile strength (Along Different Axes)

| Axis | Yield (MPa) | UTS (MPa) |
|---|---|---|
| X | 389 | 498 |
| Y | 380 | 493 |
| Z | 405 | 503 |
| 45° | 410 | 505 |
| Vertical | 393 | 499 |

The three-point bending flexural test was performed on the material using the ISO standard test specimen with dimensions 80mm x 10mm x 4mm. The three-point bending flexural test helped to determine the modulus of elasticity, flexural strain and flexural stress. Following the ASTM E290-14 standards, the bending fixture used for the testing was designed in a way that the specimens tested were bent in 'V' shape by applying pure bending force [5]. This bending test helped to determine the value of maximum flexural stress that the material can withstand. The force applied ranges from 1,000 lbs. to 1,300 lbs. or 4,448 N to 5,782N.

To understand the hardness of the 3D printed metal products, Rockwell B and Brinell Hardness tests were performed on a specimen. To understand how the additive process affects the hardness, the results from the hardness tests for the 3D printed specimen were compared with AISI 1018 – mild steel. The Rockwell scale is based on indentation hardness of a material where the penetration depth of an indenter under a large load (major load) compared to the penetration depth by a preload (minor load). Whereas, the Brinell hardness scale determines the indentation hardness through the scale of penetration of an indenter.

Table 6 – Comparison of hardness test results

| Material | Rockwell B | Brinell hardness |
|---|---|---|
| SuperArc® L-50® (Printed) | 90 - 98 | 170 – 178 |
| AISI 1018 (Mild Steel) | 71 | 126 |

To check the presence of cracks and pores in the 3D printed parts/products, specimens were subjected to CANTESCO D101 as a dye penetrant. The developer used after the penetrant dye was CANTESCO P301. No cracks and pores were observed.

Further, to check for the microstructure and internal defects like pores and cavities, CT scans were performed, and the results were satisfactory show not defects and pores. X-ray inspection of the printed metal parts were also performed to check any voids or cavities. The result from X-ray inspection show no internal cavities. The results from CT scans and X-ray scans were consistent for multiple test specimens and proved that the metal parts manufactured using the Hybrid 3D Metal Printer were homogenous and had no internal defects.

## 4. CONCLUSION

The properties of parts manufactured using the Hybrid 3D Metal Printer are better than other technologies. But to keep the quality in check and maintain homogeneity in parts manufactured, it is important to optimize the quality and size of the weld bead. This can be done in real time using a feedback system which implements an optical sensor to communicate ECU. ECU can control and vary the influential welding parameters and can optimize the additive process thus reducing the lead time and improving the quality and mechanical properties. The results from Design of Experiments carried out to understand the significance of the factors affecting the additive process show that the Trim (Arc Length Control) is the most influential followed by the machine feed rate (MF). Higher feed rates tend to decrease the superiority of the weld bead. Hence, the higher the feed rates the more chances there are of developing cavities, voids, and pores [9]. The factors studied during the experiments can easily be controlled by the ECU proving that a feedback system will improve the quality and reduce the lead-time.

The mechanical properties are as important as the lead time and quality of the parts manufactured. The tensile testing results show that the values of YTS and UTS are good when compared to standard AISI 1018 mild steel/low carbon steel which has yield tensile strength of 370 MPa and UTS of 440 MPa [7]. These results are also in good agreement with the manufacturing data sheet of the materials. It is evident from the results that the Brinell hardness and Rockwell B numbers are better compared to the AISI 1018 (mild steel/low carbon steel) which are Brinell 126 and HRB 71, respectively [7]. During the three-point bending flexural test, it was found that the pure bending force required to bend the sample specimen ranges between 1000lbs to 1300lbs. The liquid penetration test, X-ray scans and CT scans shows that the 3D printed parts can achieve high degree of homogeneity and have less to no cracks and pores. These tests let us have a standpoint that the 3D printed parts exceed the expectation but also have a great scope of improvement in some areas.

## 5. REFERENCES

1. Duda, T., & Raghavan, L. V. (2016). 3D metal printing technology. IFAC-PapersOnLine, 49(29), 103.
2. MIG Wires and TIG Cut Lengths, Lincoln Electric, retrieved on 06/10/2020 https://www.lincolnelectric.com/en-us/consumables/mig-wires-and-tig-cut-lengths/Pages/mig-wires-and-tig-cut-lengths.aspx.
3. Montgomery, Douglas C. Design and analysis of experiments. John Wiley & sons, 2017.

4. ASTM, I. "ASTM E8/E8M-16a: Standard Test Methods for Tension Testing of Metallic Materials." West Conshohocken, PA, USA: ASTM International (2016).
5. American Society for Testing and Materials. Committee E-28 on Mechanical Testing. Standard Test Methods for Bend Testing of Material for Ductility. ASTM International, 2004.
6. Herzog, Dirk, Vanessa Seyda, Eric Wycisk, and Claus Emmelmann. Additive manufacturing of metals, Acta Materialia, 117 (2016): 371-392.
7. AISI 1018 Mild/low Carbon Steel Written AZoM, retrieved on 06/10/2020 https://www.azom.com/article.aspx?ArticleID=6115.
8. Arya, H. K., & Singh, K., Effect of current, voltage and travel speed on micro hardness of saw welded mild steel plate.
9. Swanand Pavanaskar, Process Optimization of Hybrid 3D Metal Printing Technology Using Design of Experiments (DOE), research Report – Problems in Mechanical Engineering, Western Michigan University.
10. Durakovic, Benjamin, Design of experiments application, concepts, examples: State of the art, Periodicals of Engineering and Natural Sciences 5, no. 3 (2017).

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 25 June 2020 |
| Article ID | iccotwt.2620 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 02 July 2020 |
| eAID | 2020.iccotwt.2620 |

# EMBEDDED IOT SYSTEMS WITH FREE RTOS

**Ishwar Rattan [1], Subramaniam Ganesan [2]**

*[1]Central Michigan University, USA*

*[2]Oakland University, USA*

**ABSTRACT:** This paper describes use of real time operating system (FreeRTOS) for IoT (Internet of things) and other applications on a small low-cost microprocessor board. The advantage of using RTOS for IoT applications is that it can be used on various heterogeneous processor-based nodes. Most of the code can be made processor independent and be moved to heterogeneous nodes. We describe briefly features of FreeRTOS, the use of real time scheduling concepts on a FRDM board and traffic signal control application. The aim of the paper is to introduce real time concepts and use of RTOS on a small embedded system board.

## I. INTRODUCTION

Real time operating systems (RTOS) provide support for deterministic timing behavior while general operating systems (OS) provide non-deterministic behavior. Real time embedded systems require very fast response and low latency dependent on the application requirement. For example, the automotive engine controller performs multiple tasks. Each task has its own timing needs. RTOS helps in scheduling these tasks using selected algorithms before their deadlines. Depending on the application the response time can vary from microseconds to hours. The hardware can have virtual memory support for the scenario when response time requirement is large but virtual memory is not suggested for very short response time case

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.

inter-task communication, timing and synchronization functionality in the core [1].

In a real-time system, a timely response to an external input is vital. It means that multiple tasks should execute before their respective deadlines. Deadline depends on the task and application environment, which is generally a specific time instant or a time interval. The task should complete or execute accurately within its deadline. Sometimes to meet the deadline, the task computation need not be accurate, but can be approximate value. In hard real time (HRT) systems the tasks have to meet the deadline all the time. If not done, there will be a catastrophic result. Example: aircraft falls down. Soft real time (SRT) systems can violate the deadlines occasionally as long as they complete. Example: There is no catastrophic result if your cell phone internet access takes more time.

## II IOT

IOT (Internet of Things), is a network of physical objects or nodes (such as wearables, home appliances, cameras, instruments, security systems etc.) embedded with smart components (such as microprocessors, sensors, actuators etc.) and connected to other devices and system over the Internet [2]. An IoT node itself is a connected device e.g. each sensor acts as a node to provide some valuable data to a control device at the edge of the IoT ecosystem. Nodes are connected to their operators or cloud via IoT gateway (a physical device or software program). RTOS is useful in IOT. IOT needs real time monitoring, analysis and control. RTOS coordinates all these activities in the IOT device. They all communicate and share data/information using stipulated protocols in order to achieve smart reorganizations, positioning, tracing, real time online monitoring, online upgrade, process control and administration. Figure 1 shows the architecture of IoT, showing how the various devices are connected to the FOG and then to the cloud. Fog uses edge computers to carry out a substantial amount of computation, provide storage, and routing communications both local and remote. Fog computing is closer to nodes where the data is created and it improves efficiency.

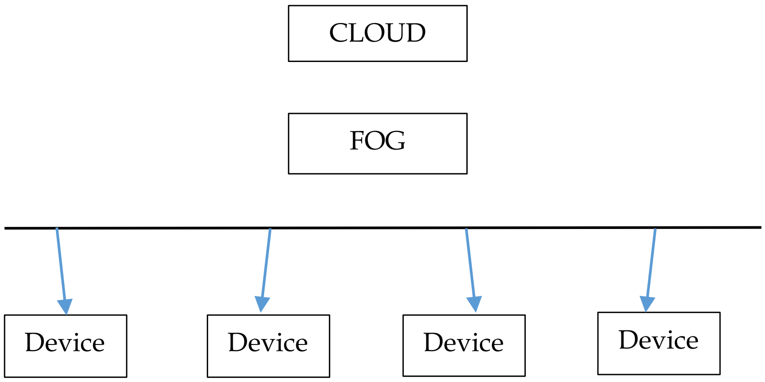


Figure 1. IOT architecture

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.

## III. RTOS

An operating system (OS) manages the hardware resources of a computer like memory allocation, interrupt servicing, and interface to input or output devices. An RTOS performs these tasks with very precise timing and a high degree of reliability. This is especially important in hard real time embedded systems where a program delay could cause a safety hazard. RTOS schedules various tasks based on the scheduling algorithms, manages message queues, semaphores, mutexes, and timers. RTOS are used in many embedded applications where there are multiple tasks with strict deadlines and priorities. A very simple embedded application may not need RTOS. The automotive anti-lock brake system is an example application for RTOS. A typical anti-lock brake system consists of an electronic controller (MCU) running RTOS, wheel speed sensors, hydraulic modulator and power source to modulate the brakes. Aim is to prevent wheel lock in slippery roads. When wheel lock is sensed or impending wheel lock is sensed, the brake is pulsed or modulated to bring the speed lower and out of the locked condition. There are three important tasks: reduce stopping distance, improve stability, and improve steerability during braking. This system receives speed information from the four-wheel speed sensors continuously, processes the data by using control logic calculations, and adjusts brake on-off pulses. The deadlines for each task is met so that the car is safe under any road conditions. RTOS ensures that the task scheduling is optimum to meet the task deadlines. RTOS are well suited for hard real time systems that require non-stop operations, and high reliability without down-time.

## IV. SCHEDULING

Scheduling various real time tasks is done using RTOS [4]. A real-time scheduling **s**ystem is composed of the scheduler, clock and the processing hardware elements. In a real-time system, the tasks should be schedulable. The tasks are accepted and completed as specified by the task deadline depending on the chosen scheduling algorithm. The scheduling can be dynamic or static. Dynamic scheduling provides efficient schedules. In a static algorithm the task running schedule is decided offline by the programmer. Static scheduling is relatively easy and provides a good analysis of the schedulability issues of multiple tasks.

A clock-driven scheduling algorithm is primarily used for hard real-time systems where all properties of all jobs are known at design time, such that offline scheduling techniques can be used. Weighted round-robin is used for scheduling real-time traffic in high-speed, switched networks. Priority-driven scheduling is used for more dynamic real-time systems with a mix of time based and/or event-based activities, where the system must adapt to changing conditions and events. For scheduling a task at a specific time, a periodic timer interrupt can be used. Decisions about what jobs execute and when to execute are made at specific time. Regular round-robin scheduling is commonly used for scheduling time-shared applications. Every job joins a FIFO queue when it is ready for execution. When the scheduler runs, it schedules the job at the head of the queue to execute for one time slice. If the job has not completed by the end of its quantum, it is preempted and placed at the end of the queue. This scheduler has limited use in real-time systems if jobs are scheduled on multiple processors. Here a job can be dispatched from the priority run queue to any of the processors. A job migrates if it starts execution on one processor and is resumed on a different processor. Static systems have lower performance (in terms of overall response time of the jobs) relative to dynamic systems. It is possible to validate a static system, whereas this is not always true for a dynamic system. Most hard-real time systems use static scheduling since it can be validated.

**EDF** - Earliest deadline first algorithm is a dynamic scheduling algorithm and it assigns priority to jobs based on deadline– Earlier the deadline, higher the priority. Priority-driven scheduling has many advantages over clock-driven scheduling. It is better suited to applications with varying time and resource requirements, as it needs less prior information and small run-time overheads. [5]

**RM** – Rate Monotonic Scheduling algorithm is very popular. Task set consists of periodic, preemptible tasks whose deadlines equal the task period. This is a static priority scheduling algorithm. Task priority is proportional to the inverse of the task period. i.e. the task with the shortest period has the highest priority.

**Precedence and Exclusion conditions** - Both RM and EDF assume that there are no precedence constraints and the tasks are preemptible. Also assumes that there is no exclusion condition—i.e. certain tasks should not interrupt certain other tasks [6].

**Multiple Runtime values for a task** - Some tasks will have two versions. Version one may execute fast and provide low quality but acceptable results. Version 2 may take more time to execute and provide higher accuracy results. The scheduler will run version 1 or version 2 depending on the workload and relative deadline.

**Sporadic Tasks** - Sporadic tasks have minimum and maximum inter-arrival time. For scheduling, they can be considered as periodic tasks with a period of minimum interarrival time. If the tasks arrive with the minimal interarrival time, they get their normal static or dynamic schedule. If the tasks come at maximum interarrival time, the scheduler does not use the slots available for the task and uses it to run some non-critical or background tasks.

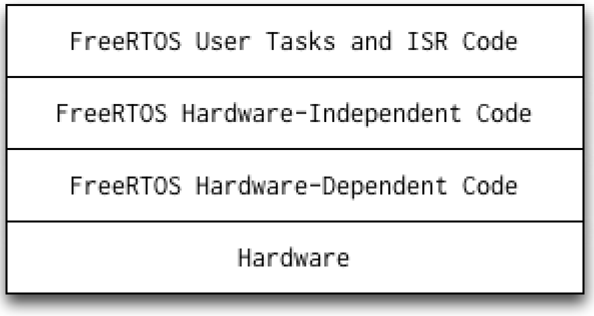
**High priority and Long period Tasks** - There may be some high priority tasks with long periods. In RM scheduling they may be assigned low priority. To increase the priority of such a task one can split the task into a number of smaller period tasks. (Example: Let task T4 have a period of 400ms, and execution time of 40 ms. To increase its priority, split it as T4′ with a period of 400/2 = 200 ms and execution time of 40/2 = 20 ms. This automatically gives higher priority for T4′ than T4. T4′ is identical to T4. Both have 40 ms execution time within 400 ms period.)

## V. **FreeRTOS**

There are a number of real time operating systems, available in the market. Some of them are: µC/OS-III, QNX, VxWorks, LynxOS, FreeRTOS, OpenRTOS, and SafeRTOS. FreeRTOS is a free, small foot-print opens-source RTOS [1]. It is simple and portable (95% of the code is in C and 5% in architecture specific assembly programming language). It has fewer bugs as compared to most RTOS (e.g. VxWorks). The salient features of FreeRTOS are: support for multiple tasks and or threads, supports both static and dynamic priority for threads, has good synchronization and communication primitives, and supports static and dynamic allocation of resources including simple memory management. It also supports scheduling of tasks with preemptive, cooperative, and hybrid scheduling algorithms. It implements a very efficient context-switch among tasks. The inter-thread synchronization supports binary, counting, recursive semaphores and mutexes (with priority inheritance to minimize priority inversion scenarios). RTOS does not support features such as device drivers, networking, file systems, user accounts, virtual memory management etc. FreeRTOS has been ported to a number of microcontroller boards (MCB), where each MCB can have one or more sensor nodes on it. FreeRTOS's code breaks down into three main areas: tasks, communication, and hardware interfacing.

- Tasks: A task is a user-defined C function with a given priority. The code in files tasks.c and task.h does creating, scheduling, and maintaining tasks.
- Communication: The code in files queue.c and queue.h handles FreeRTOS communication. Tasks and interrupts use queues to send data to each other and to signal the use of critical resources using semaphores and mutexes.

**The Hardware Whisperer:** The approximately 9000 lines of code that make up the base of FreeRTOS are hardware-independent; the same code runs whether FreeRTOS is running on an old microprocessor or the newest ARM processor. About 6% of FreeRTOS's core code acts as an  interface between the hardware-independent FreeRTOS core and the hardware-dependent code. Figure 2 shows FreeRTOS's layers. In FreeRTOS, if a static priority assignment is used (no vTaskPrioritySet() ), one can set the priorities for the tasks as per RM scheduler (task with lowest period is given highest priority).


FreeRTOS User Tasks and ISR Code
FreeRTOS Hardware-Independent Code
FreeRTOS Hardware-Dependent Code
Hardware

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.

Figure 2: FreeRTOS layers

## VI. IMPLEMENTING A TASK

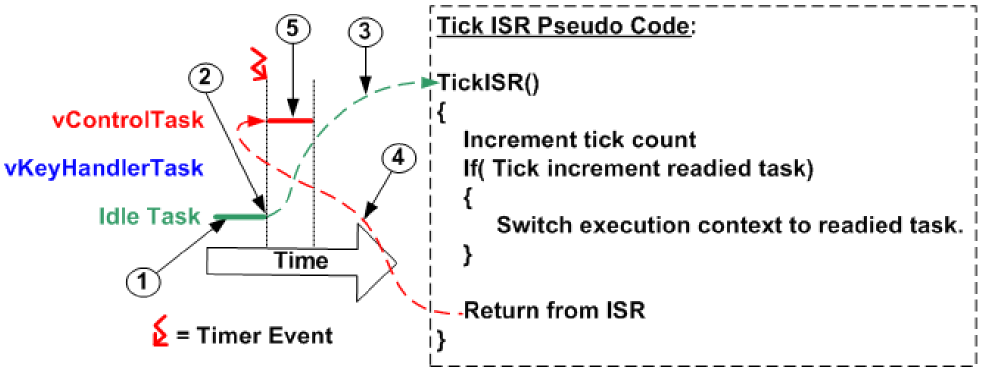
A task has the following structure:

```
void vATaskFunction( void *pvParameters )
{
   for( ;; )
   {
      -- Task application code here. --
   }
   /* Tasks must not attempt to return from their implementing
   function or otherwise exit.  In newer FreeRTOS port
   attempting to do so will result in an configASSERT() being
   called if it is defined.  If it is necessary for a task to
   exit then have the task call vTaskDelete( NULL ) to ensure
   its exit is clean. */
   vTaskDelete( NULL );
}
```

The type TaskFunction_t is defined as a function that returns void and takes a void pointer as its only parameter. All functions that implement a task should be of this type. The parameter can be used to pass information of any type into the task. Task functions should never return. Hence they are implemented as a continuous loop. Tasks are created by calling xTaskCreate() or xTaskCreateStatic(), and deleted by calling vTaskDelete().

The RTOS task will specify a time after which it requires 'waking' up when going to sleep. The RTOS task can specify a maximum time it wishes to wait when blocking. The FreeRTOS real time kernel measures time using a tick count variable. A timer interrupt (the RTOS tick interrupt) increments the tick count – allowing the real time kernel to measure time to a resolution of the chosen timer interrupt frequency. Each time the tick count is incremented the real time kernel must check to see if it is now time to unblock or wake a task. It is possible that a task woken up or unblocked by the tick ISR (Interrupt service routine) will have a priority higher than that of the interrupted task. If this is the case the tick ISR should return to the newly woken/unblocked task – effectively interrupting one task but returning to another. ISR timing is shown in Figure 3.

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.



```
Tick ISR Pseudo Code:

TickISR()
{
    Increment tick count
    If( Tick increment readied task)
    {
        Switch execution context to readied task.
    }

    Return from ISR
}
```

Figure 3: ISR timing

**Referring to the numbers in the diagram above:**

- At (1) the RTOS idle task is being executed.
- At (2) the RTOS tick occurs, and control transfers to the tick ISR (3).
- The RTOS tick ISR makes vControlTask ready to run, and as vControlTask has a higher priority than the RTOS idle task, switches the context to that of vControlTask.
- As the execution context is now that of vControlTask, exiting the ISR (4) returns control to vControlTask, which starts executing (5).

A task is preemptive if the interrupted task is preempted without suspending itself voluntarily and a context switch occurs. SafeRTOS is a safety Real Time Operating System (RTOS) for embedded systems to provide good performance and dependability, and using minimal resources[7]. It is based on the FreeRTOS functional model. One can prototype task scheduling using FreeRTOS and then convert to SafeRTOS during development.

## VII. FreeRTOS TASK CREATION

xCreateTask() function is used to create a task and add it to the ready queue. It takes 5 arguments as inputs to define various features of the task

xTaskCreate(MyTask-pointer, Task-name, StackDepth, Parameter, Priority, TaskHandle)

where MyTask-pointer: This first argument to task creation function is a pointer to a function definition of a task. Because we need to define a task with the help function.

Task-name: This argument is just the name of the function/task that we will create.

StackDepth: In multitasking, each task/thread has its own stack. It defines the stack size of a task in bytes.

Parameter: If we want to pass a pointer to a variable as an argument to the task function, we can use this argument. Otherwise, we can pass the NULL value. This argument is a pointer to a variable that the task (function) can receive.

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.

Priority: This is an important parameter because it is used to set the priority of tasks. We set priority with passing numbers as an argument. For example, if we create four tasks and assign them priority 0, 1,2 and 3. Hence, zero means the lowest priority and 3 means the highest priority.

TaskHandle: This argument keeps the handle of the function that we can use to change function features such as the deletion of a task, changing its priority, etc. We can create multiple threads by using xCreatTask.

## VIII. SETTING TASK EXECUTION PATTERN

vTaskDelayUntil function is used to define a deterministic sequence of task execution. For example, if there are four tasks to be executed after 100, 120, 130 and 140ms, vTaskDelayUntil blocks the task for a defined time after its first execution. vTaskDelayUntil is different from delay of the board. It delays a specific task and the CPU keeps executing other threads.

FreeRTOS follows both pre-emptive scheduling and cooperating scheduling. But by default, this API implements pre-emptive time-slicing scheduling. That means high priority tasks preempt low priority tasks and equal priority tasks use time-shared policy to get CPU resources. This code creates four tasks with different priorities. But all three tasks are periodic. Because of vTaskDelay() function, each task goes to a blocking state for a specified time.   The following is an example code with 3 tasks [9]

```
#include <Board_FreeRTOS.h>
void setup()
//Initialize the Serial Monitor with 9600 baud rate
{
Serial.begin(9600);
Serial.println(F("In Setup function"));
//Set the digital pins 8 to 11 as digital output pins
  pinMode(8,OUTPUT);
  pinMode(9,OUTPUT);
  pinMode(10,OUTPUT);
  pinMode(11,OUTPUT);
//Create three tasks with labels Task1, Task2 and Task3 and assign the priority as 1, 2 and 3 respectively.
//We also create the fourth task labeled as IdelTask when there is no task in
//operation and it has the highest priority.
 xTaskCreate(MyTask1, "Task1", 100, NULL, 1, NULL);
 xTaskCreate(MyTask2, "Task2", 100, NULL, 2, NULL);
```

**Cite this article as:** Rattan, I., & Ganesan, S. (2020). EMBEDDED IOT SYSTEMS WITH FREE RTOS. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-13). London, GB: ASDF International.

```
 xTaskCreate(MyTask3, "Task3", 100, NULL, 3, NULL);

 xTaskCreate(MyIdleTask, "IdleTask", 100, NULL, 0, NULL);}

//We can change the priority of task according to our desire by changing the numeric's //between
NULL texts.

void loop()

{

//There is no instruction in the loop section of the code.

// Because each task executes on interrupt after specified time

}

//The following function is Task1. We display the task label on Serial monitor.

static void MyTask1(void* pvParameters)

{

  while(1)

  {

    digitalWrite(8,HIGH);

    digitalWrite(9,LOW);

    digitalWrite(10,LOW);

    digitalWrite(11,LOW);

    Serial.println(F("Task1"));

    vTaskDelay(100/portTICK_PERIOD_MS);

  }

}

//Similarly this is task 2

static void MyTask2(void* pvParameters)

{

while(1)

  { digitalWrite(8,LOW);

    digitalWrite(9,HIGH);

    digitalWrite(10,LOW);
    digitalWrite(11,LOW);
    Serial.println(F("Task2"));
    vTaskDelay(110/portTICK_PERIOD_MS);
  }
}
//Similarly this is task 3
static void MyTask3(void* pvParameters)
{
while(1)
  {
   digitalWrite(8,LOW);
   digitalWrite(9,LOW);
   digitalWrite(10,HIGH);
   digitalWrite(11,LOW);
   Serial.println(F("Task3"));
   vTaskDelay(120/portTICK_PERIOD_MS);
  }
}
//This is the idle task which has higher priority and calls when no task is running.
static void MyIdleTask(void* pvParameters)
{
  while(1)
   {
    digitalWrite(8,LOW);
    digitalWrite(9,LOW);
    digitalWrite(10,LOW);
    digitalWrite(11,HIGH);
    Serial.println(F("Idle state"));
    delay(50);
```

```
 }
}
```

## IX. FRDM K-64 F board for IOT

FRDM- K64F board is based on ARM® Cortex®-M4 Core [8]. The FRDM K64F board has a Form-factor compatible with the Arduino R3 pin layout. It has a 6-axis digital accelerometer and magnetometer to create full eCompass capabilities, a tri-colored LED and 2 user push-buttons for direct interaction, a microSD card slot, and connectivity using onboard Ethernet port and headers for use with Bluetooth® and 2.4 GHz radio add-on modules. Figure 4 shows details of the board.

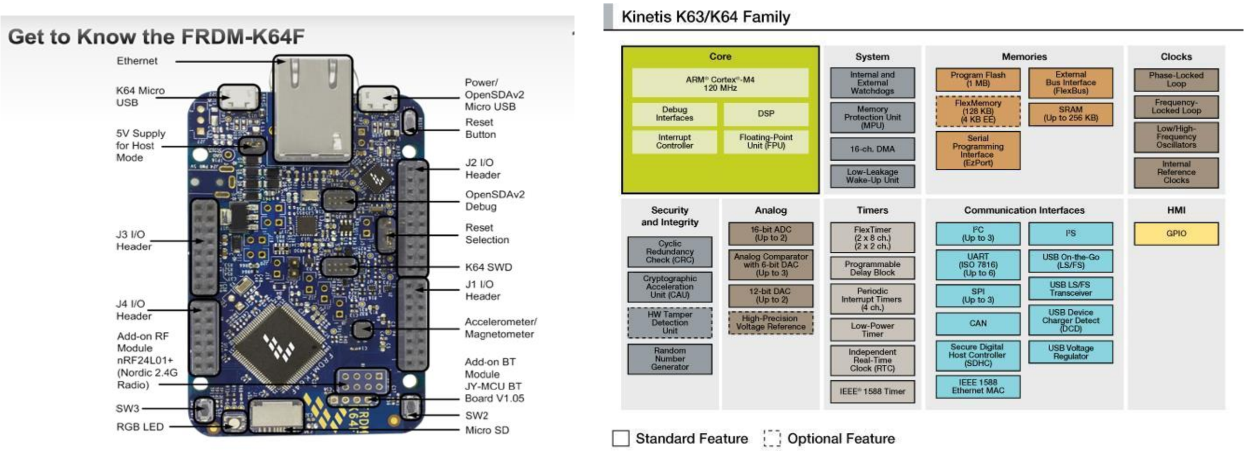


Figure 4: FRDM board details

The FreeRTOS kernel running on the FRDM board can be used to schedule multiple tasks simultaneously for many applications. The board has the Cortex-M4 a high-performance low-cost processor for applications including automotive, sensor network, medical instruments, IOT, robotics, smart city, and smart watch. The FRDM board is ideally suited for developing applications for IOT, since this board has ethernet connectivity, various sensors like accelerometer, low power consumption, low cost and analog interface. The benefits of using FreeRTOS are: Abstract out timing information, Maintainability/ Extensibility, Modularity, Cleaner interfaces, Easier testing, Code reuse, Improved efficiency, Flexible interrupt handling, and Easier control over peripherals. Some of the disadvantages of using RTOS are, the possibility of starvation of low priority tasks, and difficulty to program.

## X. APPLICATION of FreeRTOS in TRAFFIC CONTROLLER

The traffic light controller is a hard-real time system (with multiple tasks). The operating system takes into consideration which task takes priority. It assumes the following:

- All tasks are periodic
- Tasks do not synchronize with other tasks, i.e. share resources, exchange data
- Preemptive scheduling must be implemented to ensure that the CPU executes the highest priority tasks that are ready to run

FreeRTOS is a preemptive kernel and the highest priority task is always ready to execute. Interrupts or ISR will preempt tasks when called upon resulting in resuming the highest priority task once it's completed--Figure 5 illustrates this.

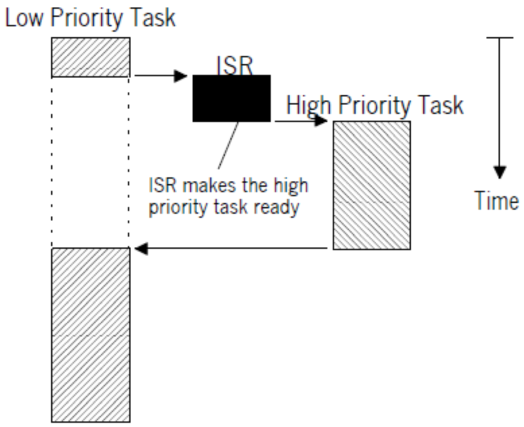


Figure 5: prioritizes tasks and interrupts

Tasks have typically never-ending looping. Tasks can be deleted when they have completed. They are more typically set as dormant when required to be active for a given time period

Code written for traffic signal application can be split into a number of tasks such as tasks for assigning period, time for each color light, priority, interrupts for pedestrian crossing requests, and camera to identify the amount of traffic in each direction and sequence. Figure 7 shows a typical traffic signal.

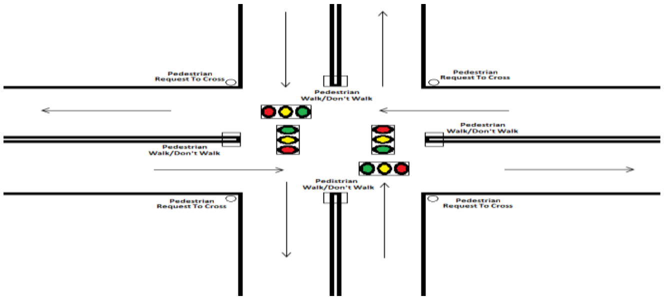

Pedestrian Request To Cross
Pedestrian Request To Cross
Pedestrian Walk/Don't Walk
Pedestrian Walk/Don't Walk
Pedestrian Walk/Don't Walk
Pedestrian Walk/Don't Walk
Pedestrian Request To Cross
Pedestrian Request To Cross

Figure 7 Traffic Signal

More sophisticated controller with more states can be designed. We describe a simple traffic controller, which is based on traffic on the road and allows pedestrians to request for "walk". The East West signal goes from Red (55 sec) to Green (55 seconds) to Yellow (5 seconds) and returns to Red. After 115 seconds, the North South traffic signal gets through the above cycle and then the control goes to East West. If there is no traffic in one direction detected by IR sensor, the signal does not return to that direction for 230 seconds. If there is a request from a Pedestrian from any corner, then the East West and North South signals (all) turn to Red and wait for 55 seconds with Walk signal on. EW signals have priority over NS signals. Once a signal goes to Green, it has to be there for 55 seconds and then turn yellow and then go to red. This action cannot be interrupted. Pedestrian request will be serviced only after a minimum of 230 second interval (i.e. the NS and EW signals are serviced once). If the pedestrian request comes during a Red signal, the duration of the red timing is increased in both directions. We have tasks with execution time, period, priority, preemption, duration during which tasks cannot be interrupted (with possible priority inversion), Cyclic schedulers (depends on traffic detection), and timer interrupts. This system can be made more efficient by adding Right turn signals and Walk for requested direction only.

## XI. CONCLUSION

In this paper, we reviewed RTOS characteristics, scheduling concepts and FreeRTOS features. We showed the use of task scheduling, use of a real time operating system, implementation on a microcontroller board and hints for writing real time software for a simple application.

## XII. REFERENCES

1. https://www.freertos.org
2. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/
3. https://en.wikipedia.org/wiki/Real-time_operating_system
4. http://et.engr.iupui.edu/~dskim/Classes/ESW5004/RTSys%20Lecture%20Note%20-%20ch03%20Overview%20of%20Real-Time%20Scheduling.pdf
5. http://et.engr.iupui.edu/~dskim/Classes/ESW5004/
6. J.Xu and D.L. Parnas, “Scheduling Processes with Release Times, Deadlines, Precedence and Exclusion Relations” IEEE trans Software engg, March 1990 (vol. 16 no. 3), pp 360-369
7. https://www.highintegritysystems.com/safertos
8. https://os.mbed.com/platforms/FRDM-K64F/
9. https://microcontrollerslab.com/use-freertos-arduino/
10. https://ops.fhwa.dot.gov/publications/fhwahop06006/chapter_12.htm-- Traffic control

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 26 June 2020 |
| Article ID | iccotwt.2627 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 03 July 2020 |
| eAID | 2020.iccotwt.2627 |

# PANDEMIC SMART BAND AN IOT BASED PRODUCT IDEA TO CONTROL THE VIRUS OUTBREAK

**Sreenivas Eeshwaroju[1], Praveena Jakkula[2] , Subramaniam Ganesan[3]**

*[1]B.Tech in ECE, Principle Engineer , [2]M.S in EEE, ECE & ISEM*

*[3]Ph.D & Senior Member IEEE,Electrical & Computer Science Engineering,Oakland University*

**ABSTRACT:** There is a potential need for efficient patient monitoring systems for the future world in increasing population and disease outbreaks. We have seen in recent times that how the COVID-19 virus spread happened and turned out as a pandemic. We are proposing an IoT based novel idea "pandemic smart band", this will help to monitor and track critical patient health and movement. This paper explains the pandemic smart band architecture, block diagram, functionality, features like hotspot tracking, Geofencing, E-Pass, fall detection, SOS, Pulse monitoring, and benefits. The main aim of this idea is to restrict the virus spread by monitoring the patient's locomotion and alert the system. This multifunctional band also acts as emergency SOS to rescue the user.

**Keywords :** Smart band, safety band, pandemic band, patient monitoring, patient tracking, IoT safety band, IoT alert system, smart ID, rescue band, SOS emergency alert system, geofencing, e-pass, fall detection, hotspot tracking, pulse monitoring.

## I. INTRODUCTION

The year 2019-2020 will be a notable year of everyone's life with the experience of major outbreak of "COVID19 -The most recent Pandemic" which has impacted almost the entire world adversely. The virus has changed lifestyle and process of almost everything in life where mask and social distancing has become

***Cite this article as:*** *Eeshwaroju, S., Jakkula, P., & Ganesan, S. (2020). PANDEMIC SMART BAND AN IOT BASED PRODUCT IDEA TO CONTROL THE VIRUS OUTBREAK. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.*

the new normal. The virus is invisible and most dangerous fact is the diseased cannot know if they are infected till several days and by then they might have unknowing spread this across to way too many people. In such scenarios it is essential to track the presence of virus and caution the nearby surroundings regarding. By now each country has taken tracing pandemic occurrence seriously and have assigned special task force to accomplish this. However, there is a need for a better, efficient and easy way to address issues like this. Which would be needed in case of any pandemic. Disease outbreaks are usually caused by either infections, contact, or any environmental changes or sometimes could be totally air borne [1]. This paper proposes an idea of Pandemic Smart Band, which are based on Internet of Things (IoT). The idea can monitor the patient's health and their movement. This band can alert the surroundings to be cautious. The architecture details and functional overview of the proposed solution is elaborated in later sections of the paper.

## II. LITERATURE REVIEW

Health bands are in general needed to help monitor the patient's health condition and take required precautions when needed and is essential to avoid fatal incidents of an individual. In case of communicable diseases, there is a need to not only monitor the health of the patient but also to track their movement to constrain the spread. Most importantly during the outbreak of deadliest diseases like COVID19, Plague or Ebola [2] many other types of influenzas [3] or in other words Pandemic outbreaks [4, 5]. The spread of the disease is like a dense spider web and having a smart band like the one proposed in this paper will aid the control of the spread and save many lives.

The consequences of pandemics lead to Health Impacts, Economic Impacts, Social and Political Impacts. Also, the treads of Pandemic risks have been increasing year after year [6, 7]. However, the existing mitigation plans so far aren't enough to cope with the situations and there is a high demand and need of more efficient ways. To withstand pandemics there is a need to build healthy nations, clean environment, reduce pollution and inculcate eco-friendly acts in all aspects of life of every individual. In addition, the preparedness is a must and with the existing technological advancements as of today that is achievable. One such attempt is this proposal where Pandemic Smart bands rely on IoT and they have the capability to monitor the health of the patient and also restrict his movements and caution him and surroundings of the presence of virus. This way the Pandemic Smart band will help contain the disease.

There has been some work done in the area of health monitoring bands, which help monitor patient's heartbeat, breath [8]. There exists research on some e-health monitoring band to diagnose patients having device implants like pacemakers and others, avoiding hospital visits [9]. However, there is need of additional features to tackle pandemics scenarios and closely monitor the spread of the disease. To address this gap and to meet the need of this pandemic situations this idea is being proposed. The elaborated details of the working of the band are illustrated in this paper.

The aim of this paper is to address the following questions with a proposed idea of an IOT based tool design which will help to contain the spread of communicable diseases and be better prepared to deal with future pandemics.

### A. Why We Need This

World had witnessed couple of pandemics so far and Asian Flu Pandemic was the one of the most widespread pandemics in history. The pandemic outbreaks happen due to wide spread of virus from one to another. We lost millions of people due to this uncontrolled outbreak COVID19 and loss is still ongoing. Lockdowns hopefully give the best results for certain extent but that may lead to rise other crisis like food and economic crisis leading to economic, social and several other disasters.

### B. Why Only Wristband

The main intention behind the molding this idea as wrist band [17] is, it will be (1) easy to wear by anyone and anytime (2) easy to operate with touch screen and single button control (3) quick to access and respond back (4) easy maintenance (5) light weight[10].

## III. IMPLEMENTATION

Pandemic smart band is an IoT based battery-operated wearable device which looks like a regular smart watch, having the capability to monitor patient health, track the movements and alert the system. This band have multiple features, explained in next sections of the paper.

### A. Functional Block Diagram

The intention behind this idea is to control the disease outbreak by monitoring the critical patient and alert the system (i.e., public, hospitals, police). Figure 1 shows the functional overview of the smart pandemic band. The main jobs of the pandemic band are (1) check the user authentication, which ensures the band is with right user (2) collects the user's health data [11], location of the user or the patient (3) Data exchange with the cloud server, cloud server enables two way communication i.e., uploads the user or patients data to the cloud and on the other side will download the guidelines and instructions to the band for the user access (4) alerts the user.

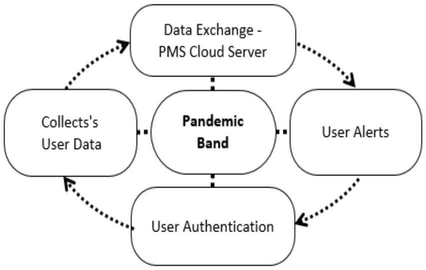


Figure 1. Functional Block Diagram

*Cite this article as:* *Eeshwaroju, S., Jakkula, P., & Ganesan, S. (2020). PANDEMIC SMART BAND AN IOT BASED PRODUCT IDEA TO CONTROL THE VIRUS OUTBREAK. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.*

### B. Module Level Block Diagram and Details

The below Figure 2 block diagram explains the electronic modules in “pandemic smart band” and interconnection.

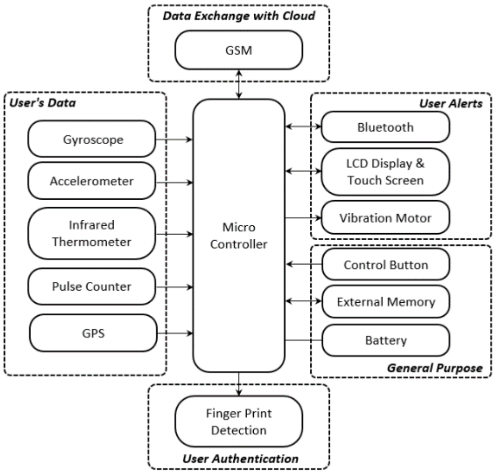


Figure 2. Electrical Block Diagram

#### a. MCU

Micro controller unit is the brain of pandemic smart band, which takes the user data, processes it, displays the data and takes necessary actions.

#### b. Liquid crystal display & Touch screen

Liquid Crystal Display acts as face of the pandemic smart band, displays the information like date, time, heart rate, user health data and guidelines for the user. Touch screen acts as input device to the smart band. User can feed the inputs manually by touching the screen and select the icons.

#### c. Control Buttons

These are multipurpose push buttons, which are required to power on and off the device, pairing Bluetooth devices and emergency SOS.

#### d. GPS Receiver

This GPS receiver [12] module helps to locate the user on the earth. Pandemic smart band will export the latitude and longitude co-ordinates in NMEA format with 10mtr accuracy (accuracy depends upon the satellite coverage)

#### e. GSM

This module is responsible to push the user’s data to the cloud and pull the alerts, guidelines from the cloud [13]

#### f. Digital Gyro Sensor

This sensor is responsible to detect the angular movement and acceleration to know the sudden displacements of the smart band [14]

### g. Bluetooth Low Energy Communication

This module enables to connect pandemic band with the external devices like smart phones. over Bluetooth.

### h. Vibration Motor

This is a compact vibration motor, small unbalanced mass on a DC motor creates vibrations when we power on motor. Microcontroller turns on and off as application demands.

### i. External Memory

External memory is an on-board memory used to store the user's health data and save the recent location details along with time stamp. This memory storage operates in FIFO model. [11]

### j. Battery

Finally, this is the most important part of the product, which enables power supply to all the modules of the smart band. This will be a rechargeable battery or batteries pack. This band will operate on low power mode to save the battery life and helps keep tracking for longer time.

## IV. APPLICATION OVERVIEW

This application is intended to monitor the critical patient's movements and alert the nearby people and take necessary actions. Pandemic band is wearable just like smart watch with extra features and aims to save the mankind. Once the patient is identified as a critical patient, patient monitoring system (PMS) will tie the pandemic band to the critical patient and keep monitoring until patient gets cured and returns to normalcy. Each pandemic band will have a unique SIM to track it individually. The standalone model can save the lives by reducing the virus spread.

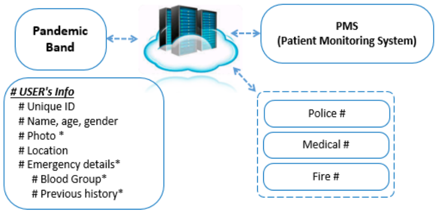


Figure 3. Pandemic band & PMS overview

### A. Account Registration

Patient monitoring system will push the user details into pandemic band and upload to the cloud server. User details comprise of the patient's personal information like complete name, fingerprints, local unique identification, home address, guardian details and medical information like blood group, disease ID, medical allergies and family physician [16]. As shown in Figure 3, patient monitoring system can monitor the critical patient details. PMS will define the boundaries where patient can move. Boundaries will vary for each band depending upon the home location, hospital areas.

***Cite this article as:*** *Eeshwaroju, S., Jakkula, P., & Ganesan, S. (2020). PANDEMIC SMART BAND AN IOT BASED PRODUCT IDEA TO CONTROL THE VIRUS OUTBREAK. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.*

### B. Categorizing Hotspots and Tracking

Hotspot categorization and tracking are the continuous process and based on user inputs. PMS server will have all the latest data points from the pandemic bands. PMS will categorise the complete area into five hotspots depends safety and allocate rank Hotspot 1 (the safest) to hotspot 5 (the most dangerous). Smart band will clearly display the current location's hotspot category.

***Hotspot #1:*** No critical patients in the zone and no one critical patient has travelled across the place.

***Hotspot #2:*** No critical patients, but critical patients had visited two weeks back

***Hotspot #3:*** No critical patients, critical patient visited within two weeks

***Hotspot #4:*** Critical patent identified and no new cases within a week

***Hotspot #5:*** More than one critical patient and new cases registered within week.

### C. Alerts and Escalations

Pandemic band is designed in such a way that it alerts the patient (level 1), guardian (level 2) and emergency services (level 3) as reporting fails shown in Figure 4

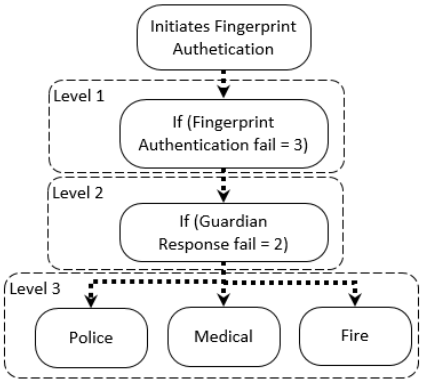

Initiates Fingerprint Authetication
Level 1
If (Fingerprint Authentication fail = 3)
Level 2
If (Guardian Response fail = 2)
Level 3
Police
Medical
Fire

Figure 4. Alerts and escalation Flow Diagram

***Level 1 Alert:*** It is vibration alert by pandemic band. This burst mode alert lasts for 7 seconds and repeats 3 times for every one-minute gap. Escalates to level 2, if the patients fail to respond back by fingerprint authentication. Vibration duration and intensity can be programmed depends on patient sensitivity.

***#Level 2 Alert:*** This is guardian alert by text message or phone call. This will notify the guardian to take necessary action. Escalates to level 3 if still patient fails to do fingerprint authentication

***#Level 3 Alert:*** This is the final alerts which informs the local emergency services ambulance, police and fire that the patient tracking is missing.

### D. Patient Recognition and Authentication

Patient recognition and authentication is an important feature to check the pandemic band is with right one and PMS is tracking the same person. This feature randomly requests the patient for fingerprint authentication. The fingerprint authentication data entered each time is verified against the preloaded patient fingerprint data entered at the time the band was initiated for the first time. The main intention of this feature is to locate the right person and restrict the movements to control the virus spread.

### E. Geofencing

This feature alerts the patient if they are trying to cross the allowed geo limits. Pandemic band calculates the safe radius from the data points fed initially and live data points received from the cloud. Patient must be within allowed limits to keep everyone safe. PMS will initiate alerts and escalation system as detailed in section 4.3 above, if patient won't follow the instructions.

### F. E-Pass

This is a multi-purpose feature of the pandemic band, where common people who aren't patients can also wear this band. This band can act as an e-pass to enter the supermarkets, shopping malls and other places. Pandemic band displays Hotspot numbers, as described in section 4.2. Only the users displaying Hotspot #1 will be allowed into the respective premises the individual

### G. Emergency SOS

This is a safety feature within the pandemic smart band for the user. User can request emergency service by pressing control button for "3 times, for more than one second duration each time" (this is called two stage protection, will be explained in later sections). Emergency centres and any speed dial contacts stored on band will be notified with the emergency notification with user's name, personal details along with location.

### H. Pulse Monitoring

Pulse monitoring is to know user health status. Figure 5 below explains the functional block diagram of Pulse monitoring and data transmission. Just like regular smart watch, the pandemic band uses an LED light to make the capillary veins in your wrist visible to a sensor that measures how fast blood is pumping, then interprets the heart rate as shown below in "beats per minute".

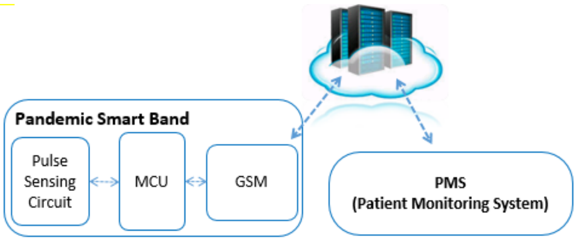


Figure 5. Pulse monitoring Functional Block Diagram

*Cite this article as:* *Eeshwaroju, S., Jakkula, P., & Ganesan, S. (2020). PANDEMIC SMART BAND AN IOT BASED PRODUCT IDEA TO CONTROL THE VIRUS OUTBREAK. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-11). London, GB: ASDF International.*

### I. Fall Detection

Pandemic smart band will detect sudden fall with the help of gyroscope and accelerometer data. It can differentiate if the user has fallen or just the smart band is dropped down. Once the event is detected, band will blink the screen trice with one second duration between each blink. If the user doesn't respond back, band assumes the user is in danger and sends the details to the emergency contacts. User can disqualify the event by pressing the control button. Figure 6 shows the functional block diagram.

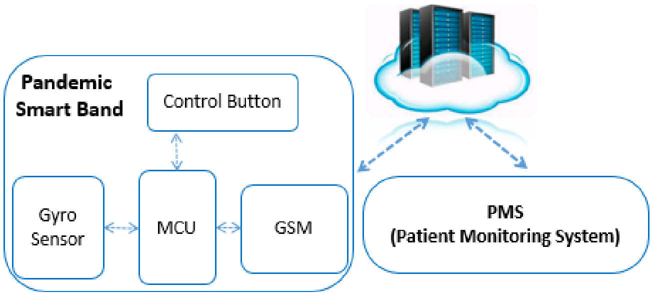


Figure 6. Fall Detection & Reporting Block Diagram

### J. System Overview

Figure 7 illustrates how the overall "smart band" system looks like. This application is mainly for immediate reporting and to get the nearby system notified of any precautions to be taken and ensure personal safety. This application can track the patient and continuously update the information to the receivers. The "smart band" system works like one of our previous publications [15].

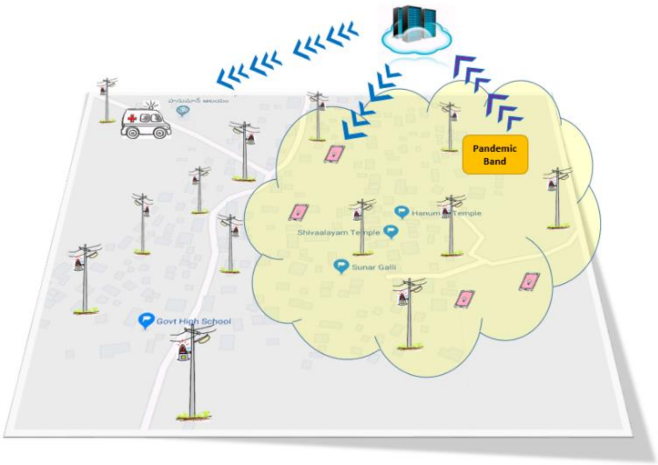


Figure 7. Pandemic Band Working Overview

## V. ADVANTAGES

There are several advantages with this standalone and automated pandemic smart band i.e., (1)It facilitates the quick and easy emergency reporting ensuring everyone's safety both the patient and people around them. This creates fearless environment and gives enough confidence. (2) Controls the virus spread by live tracking and efficient alert and escalating system (3)Only identified people will be quarantine instead complete world which will avoid several other crises like economic, trade. (4) This band can be used as general purpose band with limited and essential services which helps to keep a tab on their surroundings.

## VI. MISUSE CONTROL

The advent of technological advancements is equally enhancing the false or misuse techniques. There is a possibility that the patient doesn't wear the pandemic smart band, which can lead to dangerous outcomes. To avoid such kind of scenarios we are embedding few smart techniques to control the misuse. (1) Randomly requesting fingerprint authentication which ensures the critical patient must be alert and within the reach. (2) Ideal time calculation which calculates how long the patient did not wear the smart band. Pandemic band must be either on charging or with critical patient. (3) Over charging time calculation which measures how much extra time we kept for over charging. (4) In case the fake SOS requests from a specific device repeat multiple times, then the control station will suspend the account and there would be charges fined as a penalty. The misuse control system works like the one used in [15] i.e., the unintended or fake requests (like miss press) sent from the "smart band" to the emergency services can be minimized with a two-stage protection system.

## VII. FUTURE ENHANCEMENTS

Although the Pandemic Smart Band idea proposed in this paper is efficient, cost-effective and intelligent. There is still scope of possible enhancements like enhancing the security levels by pairing with smart devices like mobile phones, tablets. Using smart device cameras and AI (artificial intelligence) we can enhance the security levels and some of the additional. (1) CNN based facial recognition and alert system. (2) Voice based alert systems. (3) Can be used by Alzheimer's patients. (4) Private sectors can access the PMS server for the virus spread information based on location, without having access to the patient's personal details.

## VIII. CONCLUSION

This paper details on the "Pandemic Smart Band" an IOT based device idea. The design and implementation details are detailed via the block diagrams, functionality diagrams for every supported feature. This paper also illustrates the advantages, misuse control, possible future enhancements.

## IX. REFERENCES

1. Van Boeckel T P, Thanapongtharm W, Robinson T, Biradar C M, Xiao X., and others. 2012. "Improving Risk Models for Avian Influenza: The Role of Intensive Poultry Farming and Flooded Land during the 2004 Thailand Epidemic." PLoS One 7 (11): e49528. [PMC free article] [PubMed]
2. WHO (World Health Organization). 2016a. Ebola Situation Report. Weekly data report, April 15.

3. WHO (World Health Organization). 2016b. “Influenza (Seasonal).” Fact sheet, November. http://www.who.int/mediacentre/factsheets/fs211/en/.
4. WHO (World Health Organization). 2010. “What Is a Pandemic?” WHO, February 24. http://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/.
5. WHO (World Health Organization). 2016c. “Pandemic Influenza Preparedness Framework Partnership Contribution: Annual Report 2015.” Document WHO/OHE/PED/2016.01, Pandemic Influenza Preparedness (PIP) Secretariat, WHO, Geneva
6. Achonu C, Laporte A, Gardam M A. 2005. “The Financial Impact of Controlling a Respiratory Virus Outbreak in a Teaching Hospital: Lessons Learned from SARS.” Canadian Journal of Public Health 96 (1): 52–54. [PMC free article] [PubMed]
7. Barden-O’Fallon J, Barry M A, Brodish P, Hazerjian J. 2015. “Rapid Assessment of Ebola-Related Implications for Reproductive, Maternal, Newborn, and Child Health Service Delivery and Utilization in Guinea.” PLoS Currents Outbreaks (August): 7. doi:10.1371/currents.outbreaks.0b0ba06009dd091bc39ddb3c6d7b0826. [PMC free article] [PubMed]
8. S. A. Kokalki, A. R. Mali, P. A. Mundada and R. H. Sontakke, "Smart health band using IoT," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1683-1687, doi: 10.1109/ICPCSI.2017.8392000.
9. S. A. Kokalki, A. R. Mali, P. A. Mundada and R. H. Sontakke, "Smart health band using IoT," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1683-1687, doi: 10.1109/ICPCSI.2017.8392000.
10. W. Qi and Y. Zhai, "The Study on the Life Signs of Clinical Patients Monitored by Electronic Wrist Band," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, 2017, pp. 356-359, doi: 10.1109/CSE-EUC.2017.251.
11. C. Baumbauer, J. Ting, A. Thielens, J. Rabaey and A. C. Arias, "Towards Wireless Flexible Printed Wearable Sensors," 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI), Otranto, Italy, 2019, pp. 1-1, doi: 10.1109/IWASI.2019.8791367.
12. M. Shoab, K. Jain, M. Anulhaq and M. Shashi, "Development and implementation of NMEA interpreter for real time GPS data logging," 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, 2013, pp. 143-146, doi: 10.1109/IAdCC.2013.6514210.
13. Y. Lee, W. Yang and T. Kwon, "Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things," in IEEE Access, vol. 6, pp. 48994-49006, 2018, doi: 10.1109/ACCESS.2018.2859046.

14. O. Mohamed, H. Choi and Y. Iraqi, "Fall Detection Systems for Elderly Care: A Survey," 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, 2014, pp. 1-4, doi: 10.1109/NTMS.2014.6814018.
15. S. Eeshwaroju, P. Jakkula and S. Ganesan, "Rakshak – An IoT based application to address safety concerns of an Individual, Group and an Entity," ICCIT-141 conference 2020. [unpublished]
16. S. Eeshwaroju, P. Jakkula and S. Ganesan, "Smart Stick - An IoT based Product Idea for Farmers and Senior Citizens," ICCIT-141 conference 2020. [unpublished]
17. S. Eeshwaroju, P. Jakkula and S. Ganesan, "IOT based Empowerment by Smart Health Monitoring, Smart Education and Smart Jobs," ICCIT-141 conference 2020. [unpublished]

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 24 June 2020 |
| Article ID | iccotwt.2629 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 01 July 2020 |
| eAID | 2020.iccotwt.2629 |

# A MASTER'S THESIS ON HARDWARE SECURITY IN INTERNET OF THINGS (IOT)

**Ms. Sneha Subbanna[1] and Dr. Subramanian Ganesan[2]**

*[1,2]Electrical and Computer Engineering Department, Oakland University*

**ABSTRACT:** Increased applications in the field of Internet of Things (IoT) from Military to Industries and healthcare to household, has exposed the data shared between the devices in the network to extreme vulnerabilities and remote attacks. Security is a core inherent requirement to deliver safe and reliable IoT services spanning from the cloud to connected devices. IoT devices are potential entry points to wider IoT ecosystems. Thus, security of every single IoT device is more burdensome and extremely crucial. Protection of IoT devices against cyber-attacks can help achieve a high level of confidentiality, integrity, and availability with authorized access to the users. Security of IoT devices is a work in progress, and proliferation of these devices at an alarming rate is making it more challenging to secure them.

IoT security encompasses many different aspects of security such as secure boot, device authentication, encryption, secure communication, authorized transactions, and lifecycle management. Multiple software- and/or hardware-based approaches may be employed in the industry to implement security in each of these areas to meet the requirements of the specific market. Hardware-based secure elements can provide the high level of security required by many IoT applications.

Devices that are easily accessible, such as sensors and actuators are prone to physical attacks, such as being tampered with to provide incorrect data to the nodes or being sent commands from unauthorized sources. Using software security alone to protect these devices is not adequate, as the threats in these distributed systems are not confined to the software/network layer only. Without a secure hardware, the IoT devices cannot have a firm foundation to build a secure infrastructure on.

***Cite this article as:*** *Subbanna, S., & Ganesan, S. (2020). A MASTER'S THESIS ON HARDWARE SECURITY IN INTERNET OF THINGS (IOT). In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-02). London, GB: ASDF International.*

**The objective of this paper is to:**

- Highlight the challenges of IoT devices
- Emphasize the importance of IoT security
- Draw attention to the Hardware Security and importance of its implementation
- Discuss Hardware Security option

| | | | |
|---|---|---|---|
| ISBN | 978-93-88122-13-9 | VOL | 01 |
| Website | www.iccotwt.com | eMail | iccotwt@asdf.res.in |
| Received | 25 June 2020 | Accepted | 02 July 2020 |
| Article ID | iccotwt.2643 | eAID | 2020.iccotwt.2643 |

# CITY MICRO-CLIMATE DATA PORTAL

**Pallavi Tiwari**[1], **Arka Kanungo**[2]

*[1]Research Scholar, Department of Urban Planning, School of Planning and Architecture New Delhi*
*[2] Architect – Transport Planner, WSP India*

**ABSTRACT:** Cities today face a massive challenge of gap in data available for the locations of urban heat islands. The location is required for any planning intervention to offset the effect in the neighborhoods. The paper highlights a proposal is to build a web portal and mobile app, which would have updated spatial information about cities urban heat islands. The objective is to create more awareness about the pressing issue that the urban heat islands are, to deliver actionable insights for government and policy makers to take necessary actions in this regard and to provide a database to the existing NGOs working in the field to help them strategize their actions for maximum impacts.

**Key Words:** UHI, Urban Heat Islands, Interventions, Mitigation, Adaptation, Data Updation

## I. INTRODUCTION

Urban heat islands need no introduction, in the current setting of highly urbanized cities and harsh climatic conditions. The ever-increasing pressure of built up areas encroaching all the breathable spaces within the cities, the microclimatic conditions have started to deteriorate at much higher rate than it did a decade ago. Thereby creating urban heat island pockets inside the city boundaries making the harsh climate ever more un-bearable.

***Cite this article as:*** *Tiwari, P. (2020). CITY MICRO-CLIMATE DATA PORTAL. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-06). London, GB: ASDF International.*

In order to mitigate these hot spots and plan strategies to maintain a thermally comfortable outdoor condition in a more uniform way, it is first required to picture the city with respect to the land surface temperature. This is where Indian cities lack, there is no single window system or application which showcases the urban heat islands, or hot spots in Indian cities for various time periods. Planners, Urban local bodies, policy makers, and environmentalists, all can benefit if a collective and collated information about the city with its high land surface temperature zones can be identified for an efficient strategy building.

City level information is available only through published research work, state level information however is available at multiple portals. There is a requirement of city level data spatially understand the implications of human activities, physical conditions and the thermal conditions.

### Challenge

The climate is changing, and it is changing at a much rapid rate today with the advent of multiple urban risks that the cities are exposed to. The vulnerability of communities at large is globally increasing with every passing day. It is visibly affecting the environment with prominent changes and social issues pressed upon the society with the increased exposure.

The ice is melting, the sea is rising and the temperature is getting hotter day by day. To understand the global changes that occurring, one must realize the micro implication that are being faced by the population.

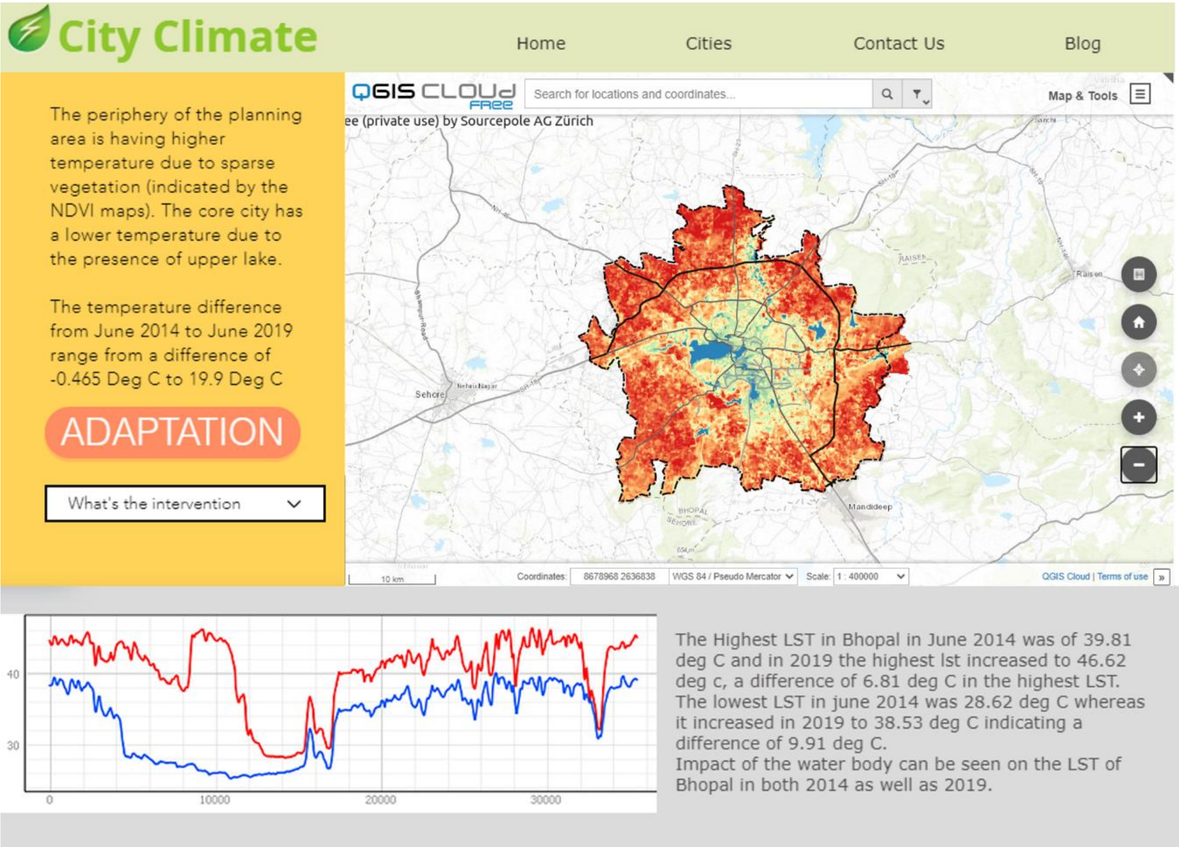
The cities are facing microclimatic changes which are more prominent than ever. Urban heat island which is defined as a metropolitan area that is significantly warmer than its surrounding rural areas due to human activities. The phenomena is not limited to a boundary of “urban” and “rural” but has over the years and with the complicated intermix of activities and spaces in the urban centers, have transitioned to a more varied heat island distribution within an urban area itself.

In order to mitigate these hot spots and plan strategies to maintain a thermally comfortable outdoor condition in a more uniform way, it is first required to picture the city with respect to the land surface temperature. This is where Indian cities lack, there is no single window system or application which showcases the urban heat islands, or hot spots in Indian cities for various time periods. Planners, Urban local bodies, policy makers, and environmentalists, all can benefit if a collective and collated information about the city with its high land surface temperature zones can be identified for an efficient strategy building. City level information is available only through published research work, state level information however is available at multiple portals. There is a requirement of city level data spatially understand the implications of human activities, physical conditions and the thermal conditions.

***Cite this article as:*** *Tiwari, P. (2020). CITY MICRO-CLIMATE DATA PORTAL. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-06). London, GB: ASDF International.*

## II. SOLUTION

The proposal is to build a web-based portal and a mobile application. This application would show in interesting graphics (easy to understand by non-technical people) about the cities microclimatic conditions and how it has been changing and by what rate or degree. The portal would also indicate remedial measures and their outcomes if implemented (i.e. if tree plantation is done in an area how much would it affect the land surface temperature or if a water body is introduced what would be the impact). The portal would act as a decision support system and would give actionable insights to climate sensitive enthusiasts, NGO's, government organizations and private organizations. City planners would benefit with this platform in terms of having data about the heat island locations in a city and reducing the existing data gap in this sector.



The periphery of the planning area is having higher temperature due to sparse vegetation (indicated by the NDVI maps). The core city has a lower temperature due to the presence of upper lake.

The temperature difference from June 2014 to June 2019 range from a difference of -0.465 Deg C to 19.9 Deg C

What's the intervention

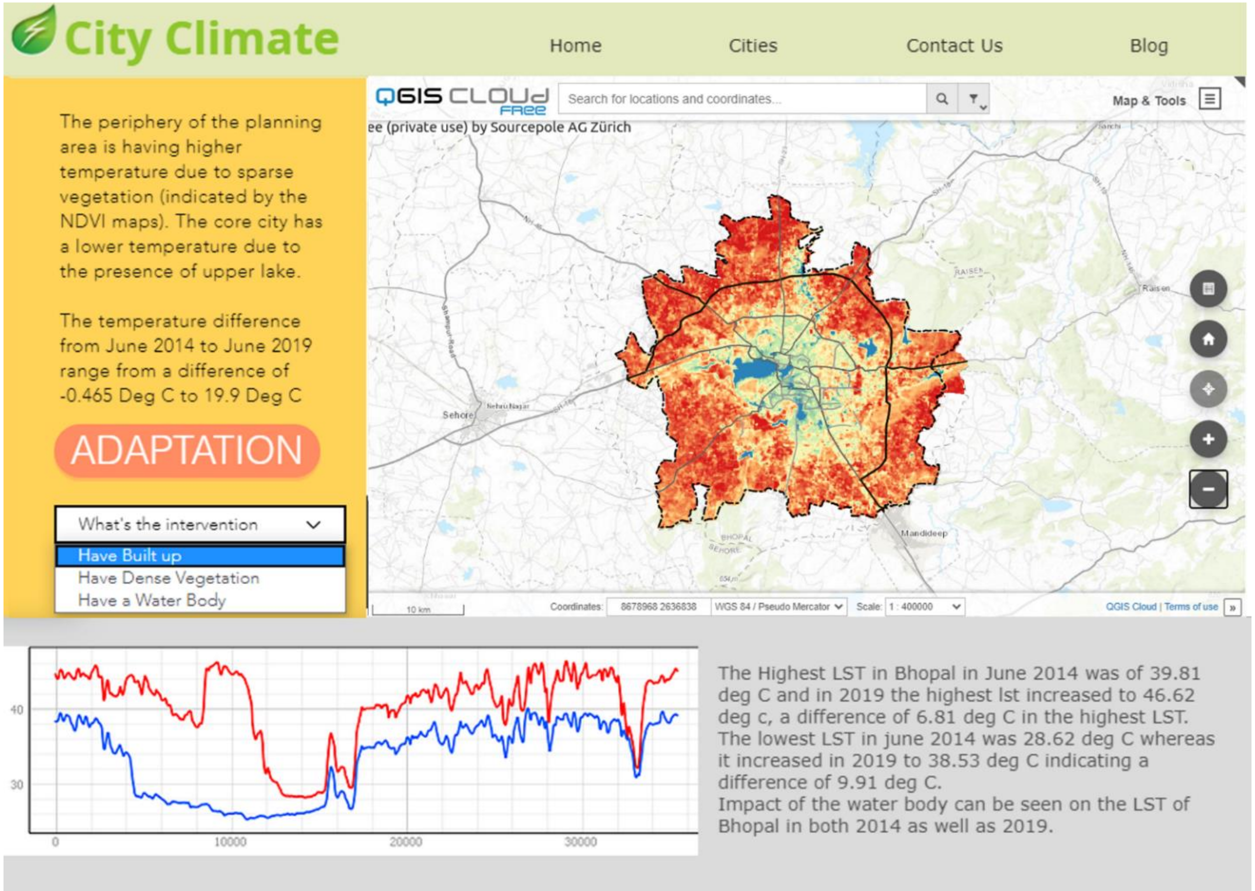
Coordinates: 8678968 2636838 WGS 84 / Pseudo Mercator Scale: 1 : 400000

The Highest LST in Bhopal in June 2014 was of 39.81 deg C and in 2019 the highest lst increased to 46.62 deg c, a difference of 6.81 deg C in the highest LST. The lowest LST in june 2014 was 28.62 deg C whereas it increased in 2019 to 38.53 deg C indicating a difference of 9.91 deg C.
Impact of the water body can be seen on the LST of Bhopal in both 2014 as well as 2019.

Figure 1 City Micro Climate CmC Data Portal Prototype

Source: Author

The prototype has been developed using the QGIS mapping platform and data generated for the city of Bhopal, India with multiple time frames. CmC portal has this data embedded as a pilot project for the proof of concept. The tab of cities consists of a city list for which the data for land surface temperature is available. The page is designed with a map window, a left detail panel, and a bottom graph panel. The map window consists of a web map (web map allows for real-time updation of data through QGIS mapping software), with features like search, zoom, map and tools, legends and coordinate details along with a base map. The left detail panel gives a brief information about the city, the time frame of the land surface calculation and the differences observed within these time frames. The same panel also has an adaptation feature which includes a drop own menu of different actions that can be introduced within the city. When one action is selected the portal displays the subsequent land surface temperature change. The actions listed included: have built up, have dense vegetation, and have a water body. The relationship has been established by multiple random points chosen to formulate a co-relation equation for each city integrated in the system. This equation is city specific calculated and integrated into the portal so as to have the most precise prediction of the impact on the city's micro climate with respect to the temperature for any intervention.



The periphery of the planning area is having higher temperature due to sparse vegetation (indicated by the NDVI maps). The core city has a lower temperature due to the presence of upper lake.

The temperature difference from June 2014 to June 2019 range from a difference of -0.465 Deg C to 19.9 Deg C

The Highest LST in Bhopal in June 2014 was of 39.81 deg C and in 2019 the highest lst increased to 46.62 deg c, a difference of 6.81 deg C in the highest LST. The lowest LST in june 2014 was 28.62 deg C whereas it increased in 2019 to 38.53 deg C indicating a difference of 9.91 deg C.
Impact of the water body can be seen on the LST of Bhopal in both 2014 as well as 2019.

Figure 2 City micro Climate Data Portal Prototype with interventions impact

Source: Author

*Cite this article as:* *Tiwari, P. (2020). CITY MICRO-CLIMATE DATA PORTAL. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-06). London, GB: ASDF International.*

**Impact**

There is a need to have a portal like the City micro Climate Data portal so as to have a data bank pertaining to the land surface temperature pattern for different cities. This information can then be used by planners, decision makers, environmentalists and climate change thinkers to come up with strategies that can be planned in cities to offset the increasing land surface temperatures. Actions can be planned in a spatial data driven priority and result oriented approach using the data provided in the portal.

**Method**

The methodology adopted for the generation of land surface temperature is as follows:

TOA (Top of Atmospheric) spectral radiance

$$\text{TOA (L)} = \text{ML} * \text{Qcal} + \text{AL}$$

**where:**

ML = Band-specific multiplicative rescaling factor from the metadata (Radiance_Mult_Band_x, where x is the band number). Qcal = corresponds to band 10. AL = Band-specific additive rescaling factor from the metadata (Radiance_Add_Band_x, where x is the band number).

TOA to Brightness Temperature conversion

$$\text{BT} = (\text{K2} / (\ln (\text{K1} / \text{L}) + 1)) - 273.15$$

**where:**

K1 = Band-specific thermal conversion constant from the metadata (K1_Constant_Band_x, where x is the thermal band number). K2 = Band-specific thermal conversion constant from the metadata (K2_Constant_Band_x, where x is the thermal band number).

L = TOA

Calculate the NDVI

$$\text{NDVI} = (\text{Band 5} - \text{Band 4}) / (\text{Band 5} + \text{Band 4})$$

Calculate the proportion of vegetation Pv

$$\text{Pv} = \text{Square} ((\text{NDVI} - \text{NDVImin}) / (\text{NDVImax} - \text{NDVImin}))$$

Calculate Emissivity ε

$$\varepsilon = 0.004 * \text{Pv} + 0.986$$

Calculate the Land Surface Temperature

$$\text{LST} = (\text{BT} / (1 + (0.00115 * \text{BT} / 1.4388) * \text{Ln}(\varepsilon)))$$

Calculation of urban heat island intensity

$$UHI = \mu + \sigma / 2$$

In which μ is the mean LST value of the study area, and σ is the standard deviation of the LST.

*Cite this article as:* *Tiwari, P. (2020). CITY MICRO-CLIMATE DATA PORTAL. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-06). London, GB: ASDF International.*

The layer of UHI is a raster layer which is symbolized to make it more understandable to be used in a portal. Random points are created in QGIS software over this raster file and the spatial join is performed with the values of NDVI, LST, Built up and NDWI. This spatial join gives a holistic data set to be used to generate a co-relation between all the parameters further used to make a predictive model. The equation with $R^2$ is then integrated in the portal.

## III. WAY FORWARD

The portal although addresses to the existing data gap. There is a possibility of further enhancing the same with the approach that solutions or actions for the offsetting of Urban Heat Islands can be of varied time durations. There can be short term, as well as long term solutions with the impact timing also different in different cases. This temporal aspect can be integrated in the intervention section of the portal to facilitate better judgment of the actions and the subsequent impact that these actions would have on the neighboring areas.

## ACKNOWLEDGMENT

The author acknowledges the existing research as an inspiration for the paper. The portal prototype has been developed using the wix website development platform along with QGIS software for all the required mapping work.

## REFERENCES

[1]. Javed Mallick, Y. K. (2008). Estimation of land surface temperature over Delhi usingLandsat-7 ETM+. J. Ind. Geophys. Union , 131-140.

[2]. Jeevalakshmi. D, D. S. (2017). Land Surface Temperature Retrieval from LANDSAT data using Emissivity Estimation. International Journal of Applied Engineering Research, 9679-9687.

[3]. Ramachandra T. V., B. H. (2012). Land Surface Temperature Analysis in an Urbanising Landscape through MultiResolution Data. Journal of Space Science & Technology, 1-10.

[4]. S.B. Ali, S. P. (2017). Microclimate land surface temperatures across urban land use/land cover forms. Global J. Environ. Sci. Manage, 231-242.

[5]. Sun, Y. (n.d.). Retrieval and Application of Land Surface Temperature.

[6]. Ugur Avdan, G. J. (2016). Algorithm for Automated Mapping of Land Surface Temperature Using LANDSAT 8 Satellite Data. Journal of Sensors.

[7]. Patnaik, S; Ali, S.B., 2018. Parks and Gardens of Bhopal: Development and attributes of urban green space in the city, Urban India 37(2).

[8]. Ali, S.B.; Patnaik, S., 2017. Thermal comfort in urban open spaces: Objective assessment and subjective perception study in tropical city of Bhopal, India, Urban Climate.

| ISBN | 978-93-88122-13-9 |
|---|---|
| Website | www.iccotwt.com |
| Received | 26 June 2020 |
| Article ID | iccotwt.2650 |

| VOL | 01 |
|---|---|
| eMail | iccotwt@asdf.res.in |
| Accepted | 03 July 2020 |
| eAID | 2020.iccotwt.2650 |

# CLOUD COMPUTING IN INTERNET OF THINGS AND NEED FOR SECURITY

**Ms. Sneha Subbanna[1] and Dr. Subramanian Ganesan[2]**

[1,2]*Electrical and Computer Engineering Department Oakland University*

**ABSTRACT:** This work in progress paper talks about the concepts of Internet of Things (IoT), architecture of different computations used for IoT applications such as Cloud, Fog, Mist and Edge, Industrial Internet of Things (IIoT) and challenges faced in IoT. Going further, this paper will discuss about the challenges faced in IoT security issues, Cyber Security and Hardware security and its implementation.

## ACKNOWLEDGEMENT

If this paper is success it is because of constant support of Dr. Subramaniam Ganesan who is my Guide for my Master's Thesis and also my professor at Oakland University. I would also like to thank the entire staff of Electrical and Computer Science department of Oakland University for their support. I would like to dedicate my work to the entire library staff of Kresge library in Oakland University for providing me access to all the resources that I required for my paper and IEEE for taking immediate action in solving issues I faced while I was trying to access the website for few references.

***Cite this article as:*** *Subbanna, S., & Ganesan, S. (2020). CLOUD COMPUTING IN INTERNET OF THINGS AND NEED FOR SECURITY. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-31). London, GB: ASDF International.*

## INTRODUCTION

Increased applications in the field of Internet of Things (IoT) from Military to Industries and healthcare to household, has exposed the data shared between the devices in the network to extreme vulnerabilities and remote attacks. Security is a core fundamental requirement to deliver safe and reliable IoT services extend over the cloud to connected devices. IoT devices are potential entry points to larger IoT networks. Thus, security of every single IoT device is more burdensome and extremely crucial. Protection of IoT devices against cyber-attacks can help achieve a high level of confidentiality, integrity, and availability with authorized access to the users. Security of IoT devices is a work in progress, and proliferation of these devices at an alarming rate is making it more challenging to secure them.

IoT security encompasses many different aspects of security such as secure boot, device authentication, encryption, secure communication, authorized transactions, and lifecycle management. Multiple software- and/or hardware-based approaches may be employed in the industry to implement security in each of these areas to meet the requirements of the specific market. Hardware-based secure elements can provide the high level of security required by many IoT applications.

Devices that are easily accessible, such as sensors and actuators are prone to physical attacks, such as being tampered with to provide incorrect data to the nodes or being sent commands from unauthorized sources. Using software security alone to protect these devices is not adequate, as the threats in these distributed systems are not confined to the software/network layer only. Without a secure hardware, the IoT devices cannot have a firm foundation to build a secure infrastructure on. The objective of this thesis is to:

- Highlight the challenges of IoT devices
- Emphasize the importance of IoT security
- Draw attention to the Hardware Security and importance of its implementation
- Discuss Hardware Security option

## INTRODUCTION TO INTERNET OF THINGS (IOT)

Imagine a world where billions of objects can sense, communicate, and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analyzed, and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of the Internet of Things (IoT).

The term Internet of Things is 21 years old. But the actual idea of connected devices had been around longer, at least since the 70s. Back then, the idea was often called “embedded internet” or “pervasive computing”. But the actual term “Internet of Things” was coined by Kevin Ashton in 1999 during his work at Procter&Gamble.

Internet of things (IoT) is a network of physical objects. The internet has evolved from being a network of computers to network of all devices of all sizes and shapes , vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected ,all communicating & sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safe & control & even personal real time online monitoring , online upgrade, process control & management.

**IoT can be defined in three categories as below**:

(1) People to people

(2) People to machine /things

(3) Things /machine to things /machine, Interacting through internet.

**Vision of IoT**: Internet of things is a conceptual model which connects all the things or the objects present in a network to other things or objects in the same network through unique addressing and wiring/wireless schemes to provide services and applications via interaction to reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities, and many other areas more intelligent.

Internet of Things is refer to the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable through information sensing device and/or controllable via the Internet, irrespective of the communication means (whether via RFID, wireless LAN, wide area networks, or other means). Everyday objects include not only the electronic devices that are encounter or the products of higher technological development such as vehicles and equipment but things that are not ordinarily considered as electronic at all - such as food , clothing ,chair, animal, tree, water etc (1).

Internet of Things is a new transformation of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things, or they can be components of complex services. This transformation is concomitant with the emergence of cloud computing capabilities and the transition of the Internet towards IPv6 with an almost unlimited addressing capacity. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service.

## HISTORY OF INTERNET OF THINGS

The Internet of Things (IoT) has not been around for very long. However, there have been visions of machines communicating with one another since the early 1800s. Machines have been providing direct communications since the telegraph (the first landline) was developed in the 1830s and 1840s. The Internet, itself a significant component of the IoT, started out as part of DARPA (Defense Advanced Research

Projects Agency) in 1962, and evolved into ARPANET in 1969. In the 1980s, commercial service providers began supporting public use of ARPANET, allowing it to evolve into our modern Internet. Global Positioning Satellites (GPS) became a reality in early 1993, with the Department of Defense providing a stable, highly functional system of 24 satellites (2).

IoT's roots can be traced back to the Massachusetts Institute of Technology (MIT), from work at the Auto-ID Center. Founded in 1999, this group was working in the field of networked radio frequency identification (RFID) and emerging sensing technologies (3). Kevin Ashton believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things. He concluded if all devices were "tagged," computers could manage, track, and inventory them. To some extent, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes. Inventory control is one of the more obvious advantages of the Internet of Things. Simply stated, the Internet of Things consists of any device with an on/off switch connected to the Internet. (2) In the 1990s, Internet connectivity began to proliferate in enterprise and consumer markets but was still limited in its use because of the low performance of the network interconnect. In the 2000s Internet connectivity became the norm for many applications and today is expected as part of many enterprise, industrial and consumer products to provide access to information. However, these devices are still primarily things on the Internet that require more human interaction and monitoring through apps and interfaces. The true promise of the IoT is just starting to be realized – when invisible technology operates behind the scenes dynamically responding to how we want "things" to act. (4)

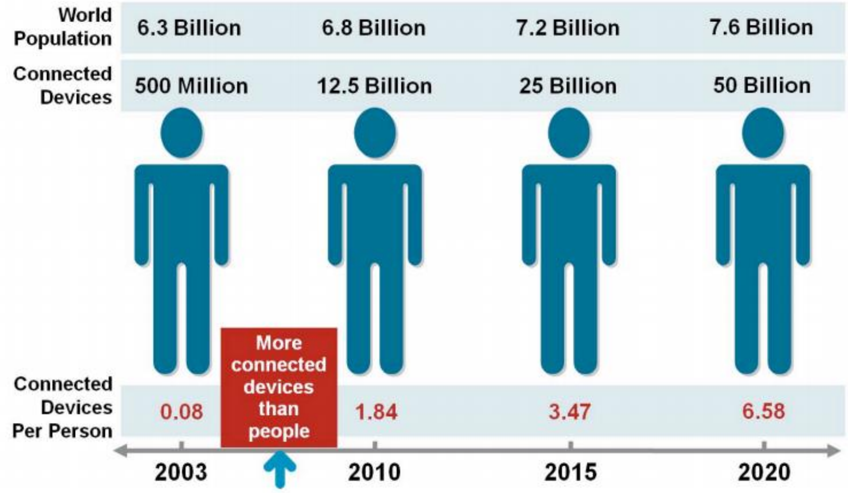


Figure 1: IoT Introduction

In 2003, there were approximately 6.3 billion people living on the planet and 500 million devices connected to the Internet. By dividing the number of connected devices by the world population it is clear that there was less than one (0.08) device for every person. Explosive growth of smartphones and tablet PCs brought the number of devices connected to the Internet to 12.5 billion in 2010, while the world's human population increased to 6.8 billion, making the number of connected devices per person more than 1 (1.84 to be exact). (3)

## ARCHITECTURE

Architecture in the IoT Domain, as any other IT domain, provides a common language to different components and stakeholders in a system. There are three basic layers of IoT architecture-

1. The client side (IoT Device Layer)
2. Operators on the server side (IoT Getaway Layer)
3. A pathway for connecting clients and operators (IoT Platform Layer)

Addressing all the layers is very crucial for an IoT device. And hence these layers are tackled in the basic four stages of IoT Architecture below-

- **Sensors and Actuators**: Sensing and actuating stage covers and adjusts everything needed in the physical world to gain the necessary insights for further analysis.
- **Internet getaways and Data Acquisition Systems**: This stage processes the enormous amount of information collected on the previous stage and squeeze it to the optimal size for further analysis.
- **Edge IT**: Edge IT systems perform enhanced analytics and pre-processing and transfers data to IT world
- **Data center and cloud**: It enables in-depth processing, along with a follow-up revision for feedback. (5)

An IoT Devices make up a physical or perceptual IoT layer and typically include sensors, actuators, and other smart devices. One might call these the "Things" in the Internet of Things. Devices, in turn, interface and communicate to the cloud via wire or localized Radio Frequency (RF) networks. This is typically done through gateways. Often IoT devices are said to be at the "edge" of the IoT network and are referred to as "edge nodes". When selecting a device, it is important to consider requirements for specific I/O protocols and potential latency, wired or RF interfaces, power, ruggedness and the device's overall sensitivity. It is critical to determine how much device flexibility your architecture should have.

IoT Gateways are an important middleman element that serves as the messenger and translator between the cloud and clusters of smart devices. They are physical devices or software programs that typically run from the field near the edge sensors and other devices. Large IoT systems might use a multitude of gateways to serve high volumes of edge nodes. They can provide a range of functionality, but most importantly they normalize, connect and transfer data between the physical device layer and the cloud. In fact, all data moving between the cloud and the physical device layer goes through a gateway. IoT gateways are sometimes called "intelligent gateways" or "control tiers". It is becoming common practice to implement data encryption and security monitoring on the intelligent gateway so as to prevent malicious man-in-the-middle attacks against otherwise vulnerable IoT systems.

**These are these requirements for an end-to-end IoT architecture,**

- Concurrent Data Collection – support for collection, analysis, and control from a large number of sensors or actuators
- Efficient Data Handling – minimize raw data and maximize actionable information
- Connectivity and Communications – provide network connectivity and flexible, robust protocols support between sensors/actuators and the cloud
- Scalable – scale individual elements in the system using the same architecture
- Security – end to end encryption and monitoring
- Availability and Quality of Service – minimal latencies and fault tolerant
- Modular, Flexible and Platform-independent – each layer should allow for features, hardware, or cloud infrastructure to be sourced from different suppliers
- Open Standards and Interoperable – communication between the layers should be based on open standards to ensure interoperability
- Device Management – enable automated/remote device management and updates
- Defined APIs – each layer should have defined APIs that allow for easy integration with existing applications and integration with other IoT solutions (6)

There are many categories of IoT architectures like Three (Layer) Tire, Five (Layer) Tire, Fog Computing, Edge Computing, Hybrid Cloud-Fog-Mist Computing, Mist, and many more domain specific architectures like Radio Frequency IDentification (RFID) , Service Oriented Architecture (SOA), Wireless Sensor Network (WSN), Supply chain Management (SCM), Health Care, Smart Society, and many more. Though there are many sorts of IoT architecture, this thesis explores Fog computing, Edge Computing and Mist Computing mainly.

Sensors, actuators, compute servers, and the communication network form the core infrastructure of an IoT framework.

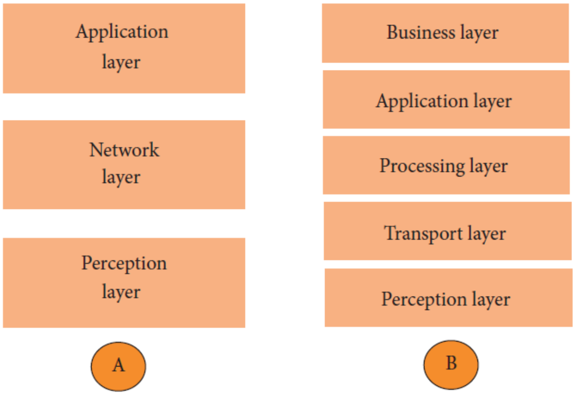


Figure 2: (A) Three layered IoT Architecture (B) Five layered IoT Architecture

This architecture was introduced in the early stages of research and the three layers are namely, the perception, network, and application layers.

- **The perception layer** is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
- **The network layer** is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
- **The application layer** is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

The Three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. One is the five-layer architecture, which additionally includes the processing and business layers.

The Five-layers are perception, transport, processing, application, and business layers. The role of the perception and application layers is the same as the architecture with Three-layers. The outline of the functions of the remaining three layers.

- **The transport layer** transfers the sensor data from the perception layer to the processing layer and vice-versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.
- **The processing layer** is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.
- **The business layer** manages the whole IoT system, including applications, business and profit models, and users' privacy. (7)

## CLOUD COMPUTING:

During 1950s, companies started to use large mainframe computers, but it was too expensive to buy a computer for each user. So, during the late 1950s and early 1960s, a process called time-sharing was developed to make more efficient use of expensive processor time. Time-sharing enabled users to access numerous instances of computing mainframes simultaneously, maximizing processing power and minimizing downtime. As computers became more diffused, scientists and technologists explored ways to make large-scale computing power available to more users through time-sharing. They experimented with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users. The idea of time sharing represents the first use of shared computing resources, the foundation of modern cloud computing.

In the 1970s, cloud computing began taking a more tangible shape with the introduction of the first virtual machines, allowing users to run more than one computing system within a single physical setup. The functionality of these virtual machines led to the concept of virtualization, which had a major influence on the progress of cloud computing. In the 1970s and 1980s, Microsoft, Apple and IBM developed technologies that enhanced the cloud environment and advanced the use of the cloud server and server hosting (8). In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service, but at a lower cost. By switching traffic as they saw fit to balance server use, they could use overall network bandwidth more effectively. They began to use the cloud symbol to denote the demarcation point between what the provider was responsible for and what users were responsible for. Cloud computing extended this boundary to cover all servers as well as the network infrastructure (9). Then in 1999, Salesforce became the first company to deliver business applications from a website (8).

Cloud computing is the delivery of computing services like servers, storage, databases, networking, software, analytics, and intelligence over the Internet (the cloud) to offer faster innovation, flexible resources, and economies of scale. The user typically pays only for cloud services used, which helps to lower the operating costs, run infrastructure more efficiently, and scale as customers' business needs change (10). A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services. Cloud infrastructure involves the hardware and software components required for proper implementation of a cloud computing model. Cloud computing can also be thought of as utility computing, or on-demand computing. A cloud service has three distinct characteristics that differentiate it from traditional web hosting,

- Users can access large amounts of computing power on demand. It is typically sold by the minute or the hour.
- It is elastic -- a user can have as much or as little of a service as they want at any given time.
- The service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed internet, have accelerated interest in cloud computing.

**Different Cloud Computing deployments:**

- **Private cloud:** Private cloud services are delivered from a business's data center to internal users. With a private cloud, an organization builds and maintains its own underlying cloud infrastructure. This model offers the versatility and convenience of the cloud, while preserving the management, control, and security common to local data centers. Common private cloud technologies and vendors include VMware and OpenStack.
- **Public cloud**: In the Public cloud model, a third-party cloud service provider delivers the cloud service over the internet. Public cloud services are sold on demand, typically by the minute or hour, though long-term commitments are available for many services. Customers only pay for the CPU cycles, storage, or bandwidth they consume. Leading public cloud service providers include Amazon Web Services (AWS), Microsoft Azure, IBM, and Google Cloud Platform.
- **Hybrid cloud:** A Hybrid cloud is a combination of public cloud services and an on-premises private cloud, with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud and use the public cloud to handle workload bursts or spikes in demand. The goal of a hybrid cloud is to create a unified, automated, scalable environment that takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.
- **Multi-cloud:** In addition, organizations are increasingly embracing a Multi-cloud model, or the use of multiple IaaS (Infrastructure as a Service) providers. This enables applications to migrate between different cloud providers or to even operate concurrently across two or more cloud providers.

**Community cloud:** A Community cloud, which is shared by several organizations, supports a particular community that shares the same concerns, (e.g., the same mission, policy, security requirements and compliance considerations). A community cloud is either managed by these organizations or a third-party vendor and can be on or off premises.

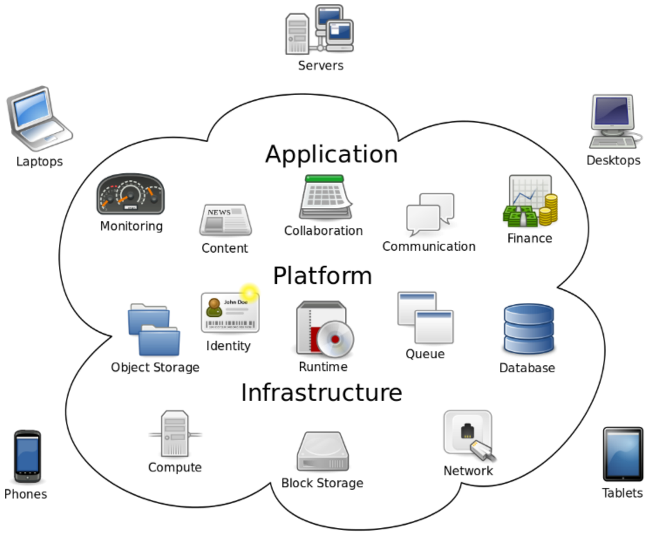


Figure 3: Cloud Computing

**Cloud computing benefits:**

- **Cost savings**: Using cloud infrastructure can cost but the organizations do not have to spend massive amounts of money buying and maintaining equipment. This reduces the capital expenditure costs of the organization as they do not have to invest in hardware, facilities, utilities or building large data centers to accommodate their growing businesses. Additionally, companies do not need large IT teams to handle cloud data center operations because they can rely on the expertise of their cloud providers' teams. Cloud computing also cuts costs related to downtime. Since downtime rarely happens in cloud computing, companies do not have to spend time and money to fix any issues that may be related to downtime.
- **Mobility**: Storing information in the cloud means that users can access it from anywhere with any device with just an internet connection and users do not have to carry around USB drives, an external hard-drive, or multiple CDs to access their data. Users can access corporate data via smartphones and other mobile devices, enabling remote employees to stay up to date with coworkers and customers. End users can easily process, store, retrieve and recover resources in the cloud.
- **Disaster recovery**: Storing data in the cloud guarantees that users can always access their data even if their devices are inoperable. With cloud-based services, organizations can quickly recover their data in the event of emergencies, such as natural disasters or power outages.
- **Elasticity**: Companies can freely scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure, which may or may not remain active.

- **Pay-per-use**: Compute resources are measured at a granular level, enabling users to pay only for the resources and workloads they use.
- **Migration flexibility**: Organizations can move certain workloads to or from the cloud -- or to different cloud platforms - as desired or automatically - for better cost savings, or to use new services as they emerge.
- **Multi-tenancy and resource pooling**: Multi-tenancy lets numerous customers share the same physical infrastructures or the same applications, yet still retain privacy and security over their own data. With resource pooling, cloud providers service numerous customers from the same physical resources. The resource pools of the cloud providers should be very large and flexible enough so they can service the requirements of multiple customers (8).

Cloud computing can be broken down into three cloud computing models. **Infrastructure-as-a-Service** (IaaS) refers to the fundamental building blocks of computing that can be rented physical or virtual servers, storage, and networking. This is attractive to companies that want to build applications from the very ground up and want to control nearly all the elements themselves, but it does require firms to have the technical skills to be able to orchestrate services at that level. **Platform-as-a-Service** (PaaS) is the next layer up -- as well as the underlying storage, networking, and virtual servers this will also include the tools and software that developers need to build applications on top of: that could include middleware, database management, operating systems, and development tools. **Software-as-a-Service** (SaaS) is the delivery of applications-as-a-service, probably the version of cloud computing that most people are used to on a day-to-day basis. The underlying hardware and operating system are irrelevant to the end user, who will access the service via a web browser or app; it is often bought on a per-seat or per-user basis (11).

Security remains a primary concern for businesses contemplating cloud adoption, especially public cloud adoption. Public cloud service providers share their underlying hardware infrastructure between numerous customers, as the public cloud is a multi-tenant environment. This environment demands significant isolation between logical compute resources. At the same time, access to public cloud storage and compute resources is guarded by account login credentials. Many organizations bound by complex regulatory obligations and governance standards are still hesitant to place data or workloads in the public cloud for fear of outages, loss, or theft. However, this resistance is fading, as logical isolation has proven reliable, and the addition of data encryption and various identity and access management tools have improved security within the public cloud (8). Cloud computing is still at a relatively early stage of adoption, despite its long history. It is anticipated that the usage is likely to climb as organizations get more comfortable with the idea of their data being somewhere other than a server in the basement. Moving to the cloud can help companies rethink business processes and accelerate business changes (11).

## FOG COMPUTING:

In 2011, the need to extend cloud computing with fog computing emerged to cope with huge number of IoT devices and big data volumes for real-time low-latency applications. On November 19th, 2015, Cisco Systems, ARM Holdings, Dell, Intel, Microsoft, and Princeton University, founded the OpenFog Consortium to promote interests and development in fog computing (12). The cloud was supposed to be an answer but, sending the data to the cloud for analysis also poses a risk of data bottlenecks, as well as security concerns. Fog computing – a term originally coined by Cisco—is in many ways synonymous with edge computing. In contrast to the cloud, fog platforms have been described as dense computational architectures at the network's edge. While edge computing or edge analytics may exclusively refer to performing analytics at devices that are on, or close to, the network's edge, a fog computing architecture would perform analytics on anything from the network center to the edge (13).

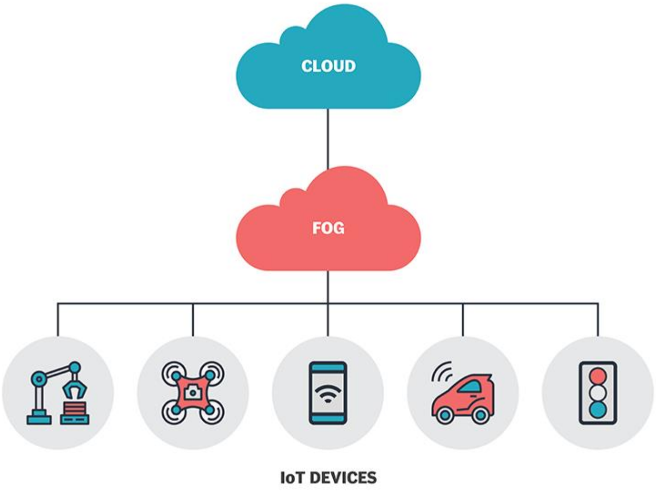


Figure 4*:* Foggy Architecture

National Institute of Standards and Technology in March 2018 released a definition of fog computing that defines fog computing as a horizontal, physical, or virtual resource paradigm that resides between smart end-devices and traditional cloud computing or data center. This paradigm supports vertically isolated, latency-sensitive applications by providing ubiquitous, scalable, layered, federated, distributed computing, storage, energy efficient, and network connectivity. Thus, fog computing is most distinguished by distance from the edge. In the theoretical model of fog computing, fog computing nodes are physically and functionally operative between edge nodes and centralized cloud. Fog computing is more energy-efficient than cloud computing (12).

**There are several reasons to support this increasing technology:**

- **Distributed architecture** – Fog Computing is known for its efficiency and zero downtime and manages to deliver the core IoT requirements such as storage and computation.
- **SCALE** (Security-Cognition-Agility-Latency-Efficiency) – These are the capabilities that place fog computing on a new level. Internet of Things requires excellent connectivity, something "foggy" architecture can provide.
- **Immersive distribution** – Fog computing can correlate not only with the cloud but with other connected devices, being able to provide resources throughout the network, not just the edge.

**And there are few business reasons which support Fog computing:**

- **Costs** – Every business owner is thinking about the costs, and how to minimize but keep the business competitive. Fog computing is a cost-efficient solution that enables efficient use of the IoT.
- **Collaboration** – It is a common framework for communication and collaboration, keeps your IoT team connected, all the time.

**Scalability** – It is also known for its shared and spread nature. In simpler terms, the architecture shreds across devices and spreads across clouds, enabling highly functioning internal business services.

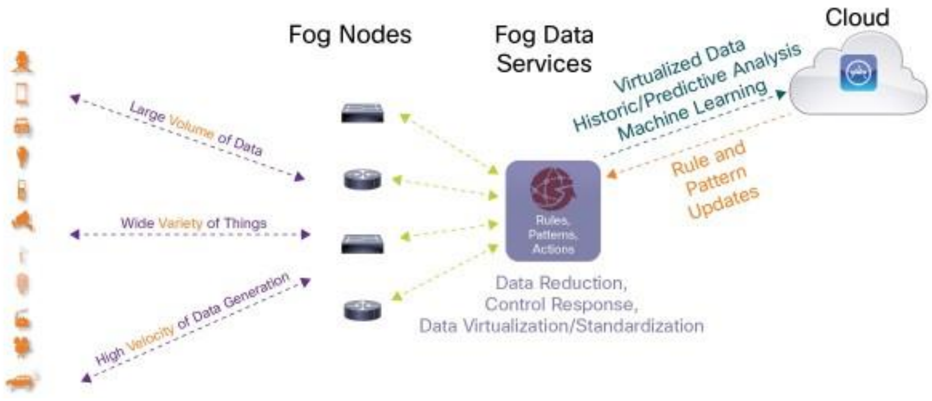


Figure 5: Fog Computing

Security is paramount for every company, and business owners have already started to design strategies to create a highly secure environment. One of the most significant advantages of fog computing is Security.

- **Ensures a high-level of protection** – Some of the IoT devices operate with minimal resources, leaving them vulnerable to sophisticated cyber-attacks. Fog Computing is built specifically for the cloud-of-things IoT security, it can ensure protection even for the smallest connected devices, such as a smart camera.

***Cite this article as:*** *Subbanna, S., & Ganesan, S. (2020). CLOUD COMPUTING IN INTERNET OF THINGS AND NEED FOR SECURITY. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-31). London, GB: ASDF International.*

- **Keep security credentials and software updates** – Fog nodes keep security credentials and software up to date on many connected devices.
- **Monitor distributed systems** – It can closely monitor all the distributed systems and devices and identify even hard-to-detect types of attacks.
- **Enable incident response without interruption** – Probably one of the most important advantages is that fog computing can detect and solve certain types of attacks without disrupting your business services (14).

Cloud computing frees the enterprise and the end user from the specification of many details. This bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements. Rather than cannibalizing Cloud Computing, Fog Computing enables a new breed of applications and services, and that there is a fruitful interplay between the Cloud and the Fog, particularly when it comes to data management and analytics. Fog Computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers, typically, but not exclusively located at the edge of network. Important Fog applications involve real-time interactions rather than batch processing. Fog nodes come in different form factors and will be deployed in a wide variety of environments. Seamless support of certain services (streaming is a good example) requires the cooperation of different providers. Hence, Fog components must be able to interoperate, and services must be federated across domains (15).

Data gathered from the devices are saved in each service separately in different format. Also, interfaces to access the resources of each service are different from each other. To populate IoT service, the interoperability between IoT services is essential. Without service-level or application-level interoperability, each service will become just another remote controller on user's smartphone and cannot provide fully connected user experience. Basically, Fog computing is an architecture to improve communication between IoT devices and IoT service and was introduced to cope with increased data flow for cloud computing. It is popular in IoT service domains which requires real-time processing in the event response such as in healthcare (16).

## EDGE COMPUTING:

With the proliferation of Internet of Things (IoT) and the burgeoning of 4G/5G network, the dawning era of the IoE (Internet of Everything) is observed. Huge volumes of data generated by things are immersed in our daily life, and hundreds of applications will be deployed at the edge to consume these data. The issues in the centralized big data processing era have helped launch a new computing paradigm, Edge Computing, which calls for processing the data at the edge of the network. Leveraging the power of cloud computing, edge computing has the potential to address the limitation of Cloud computing (17).

Edge computing is a method for optimizing cloud computing systems by performing data processing at the edge of the network, near the data source. Here the 'edge' is defined as any end device which helps in computing and acts as network resources along the path between data sources and cloud (18). The aim of Edge Computing is to move the computation away from data centers towards the edge of the network, exploiting smart objects, mobile phones or network gateways to perform tasks and provide services on behalf of the cloud. By moving services to the edge, it is possible to provide content caching, service delivery, storage and IoT management resulting in better response times and transfer rates. At the same time, distributing the logic in different network nodes introduces new issues and challenges.

Edge computing brings analytical computational resources close to the end users and therefore helps to speed up the communication speed. A well-designed edge platform would significantly outperform a traditional cloud-based system. Edge application services reduce the volumes of data that must be moved, the consequent traffic, and the distance that data must travel. That provides lower latency and reduces transmission costs. While cloud computing operates on big data, edge computing operates on "instant data" that is real-time data generated by sensors. Computation offloading for real-time applications, such as facial recognition algorithms, showed considerable improvements in response times (19). In addition, companies can save money by having the processing done locally, reducing the amount of data that needs to be processed in a centralized or cloud-based location. Edge computing was developed due to the exponential growth of IoT devices, which connect to the internet for either receiving information from the cloud or delivering data back to the cloud. And many IoT devices generate enormous amounts of data during their operations.

For many companies, the cost savings alone can be a driver towards deploying an edge-computing architecture. Companies that embraced the cloud for many of their applications may have discovered that the costs in bandwidth were higher than they expected. Increasingly, though, the biggest benefit of edge computing is the ability to process and store data faster, enabling for more efficient real-time applications that are critical to companies. Before edge computing, a smartphone scanning a person's face for facial recognition would need to run the facial recognition algorithm through a cloud-based service, which would take a lot of time to process. With an edge computing model, the algorithm could run locally on an edge server or gateway, or even on the smartphone itself, given the increasing power of smartphones. Applications such as virtual and augmented reality, self-driving cars, smart cities, and even building-automation systems require fast processing and response. With enhanced interconnectivity enabling improved edge access to more core applications, and with new IoT and industry-specific business use cases, edge infrastructure is poised to be one of the main growth engines in the server and storage market for the next decade and beyond (20).

Edge solutions are usually multi-layered distributed architectures encompassing and balancing the workload between the Edge layer, the Edge cloud or Edge network, and the Enterprise layer. Furthermore, when the Edge computing is discussed, there are the Edge devices and the local Edge servers. Edge is IoT at enormous scale because with the huge increase in devices and the data being generated by these devices, there will be bottlenecks and latency issues with current architectures. Edge computing addresses these challenges, as stated earlier in this report, by moving the processing to the edge of the network.

- **Edge devices**: The Edge and IoT devices are equipped to run analytics, apply AI rules, and even store some data locally to support operations at the Edge. The devices could handle analysis and real-time inferencing without involvement of the Edge server or enterprise layer. This is possible because devices can use any Software-as-a-Service (SaaS). Driven by economic considerations and form factors, an Edge device typically has limited compute resources.
- **Edge servers**: Edge servers are used to deploy apps to the devices. They are in constant communication with the devices by using agents installed on each of the devices. These Edge servers maintain a pulse on the plethora of devices, and if something more than inferencing is needed, data from the devices is sent to the Edge server for further analysis. These are general-purpose racked computers located in remote operations facility, like a factory, retail store, hotel, distribution center, or bank.
- **Edge Cloud**: New networking technologies have resulted in the Edge Cloud (or micro data center), which can be viewed as a local cloud for devices to communicate with. Telecommunication companies might call it the Edge network. It reduces the distance that data from the devices must travel and thus decreases latency and addresses bandwidth issues, especially with the advent of 5G. This region also offers more analytical capabilities and additional storage for analytical and data models.
- **Enterprise hybrid multicloud**: This region offers the classic enterprise-level model storage and management, device management, and especially enterprise-level analytics and dashboards. This can be hosted in the Cloud or in an on-premises data center (21).

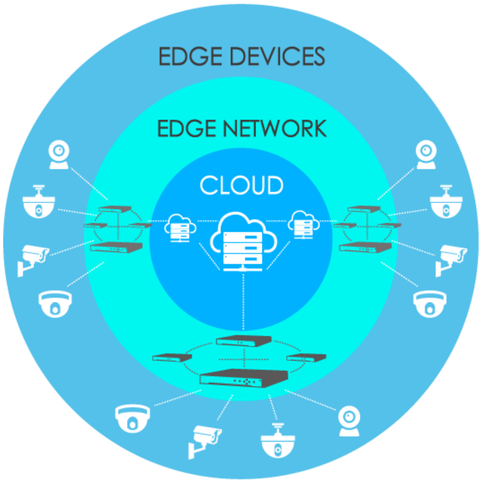


Figure 6: Architecture of Edge Computing

The more intelligent an edge device, the more intensive its configuration, deployment, and maintenance requirements. Organizations will need to decide on a case-by-case basis if distributed computing benefits justify the increased overhead at the network's periphery. Security is also a major concern associated with edge computing. Not only should data be encrypted, but different encryption mechanism should be adopted, since data may transit between different distributed nodes connected through the internet before eventually reaching the cloud. Edge nodes may also be resource constrained devices, limiting the choice in terms of security methods. Some IT professionals worry that a decentralized computing architecture will make a network more vulnerable to attack by creating excess backdoor entry points. However, other people argue that placing an edge-computing gateway between network endpoints and the internet can actually improve security. Because more data will be processed and stored locally, travel to and from the cloud will be reduced (22).

Edge computing must take into account the heterogeneity of the devices, having different performance and energy constraints, the highly dynamic condition, and the reliability of the connections, compared to more robust infrastructure of cloud data centers. Moreover, security requirements may introduce further latency in the communication between nodes, which may slow down the scaling process. Management of failovers is crucial in order to maintain a service alive. If a single node goes down and is unreachable, users should still be able to access a service without interruptions. Moreover, edge computing systems must provide actions to recover from a failure and alerting the user about the incident. To this aim, each device must maintain the network topology of the entire distributed system, so that detection of errors and recovery become easily applicable (19).

Carriers around the world are deploying 5G wireless technologies, which promise the benefits of high bandwidth and low latency for applications, enabling companies to go from a smaller data bandwidth to larger. Instead of just offering the faster speeds and telling companies to continue processing data in the cloud, many carriers are working edge-computing strategies into their 5G deployments in order to offer faster real-time processing, especially for mobile devices, connected cars and self-driving cars (20). Edge computing is more suitable to be integrated with IoT to provide efficient and secure services for a large number of end-users, and edge computing-based architecture can be considered for the future IoT infrastructure. It's clear that while the initial goal for edge computing was to reduce bandwidth costs for IoT devices over long distances, the growth of real-time applications that require local processing and storage capabilities will drive the technology forward over the coming years (23).

## Mist Computing

Mist computing is the extreme edge of a network, typically consisting of micro-controllers and sensors. Mist computing uses microcomputers and microcontrollers to feed into fog computing nodes and potentially onward towards the centralized (cloud) computing services. As fascinating as Fog computing sounds, some applications require ultra-low latency which has made people look for other options for computing power, and this computing model is known as Mist computing (24). Fog computing was introduced because it is clear that the billions of IoT devices being deployed over time cannot operate by merely having connectivity to servers, instead the computation is pushed closer to the edge of the network (gateways). The computation distribution is further distributed among the network nodes, based on their capabilities and roles with respect to the application. The microcontrollers at the edge in the majority of today's nodes have significant computational power and most of that is needed to implement their basic IoT functions. It would be better for the entire ecosystem if all the microcontrollers could provide more functionality for the network nodes.

Mist computing paradigm has decreased the latency and increased the autonomy of a solution (25). Cloud, Fog and Mist computing are complementary to each other w.r.t. the application tasks, which are more computationally intensive can be executed in the gateway of the fog layer while the less computationally intensive tasks can be executed in the edge devices. The processing and the collecting of data are still stored in the cloud data center for the availability to the user. The important application of mist computing is a collection of different services which has been distributed among the computing nodes. Both, fog computing and mist computing are coined by Cisco and located between the fog and the edge node, extend the classical client-server architecture to a more peer-to-peer based approach, similar or equal to edge (26)

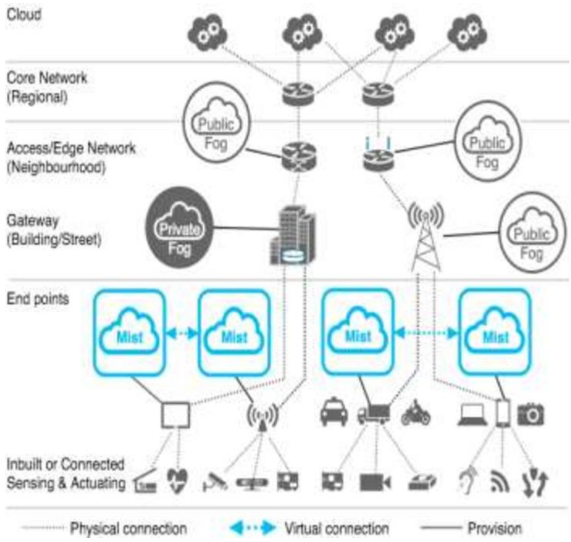


Figure 7: Mist Computation

In Mist computing the routing protocol supports direct device-to-device connectivity as sub-optimal routing paths will increase the total bandwidth requirements of the network (25). The core issue of these problems lies in the centralized nature of a cloud computing architecture. After all, only the central nodes of the network have the capability to store and process data. To combat this problem, network designers are proposing Mist computing architectures where the computing power is distributed more evenly around the network. These architectures push the processing capability out to the edge of the network, closer to the source of the data. Mist computing takes place on the ground, where it is the light computing power located at the very edge of the network, at the level of the sensor and actuator devices. Cloud, Fog and Mist computations are meant to work together and not against one another as each has its own advantages and disadvantages which can be used to design a strong computational architecture with minimal weakness.

Mist computing is all about putting computing power on the very edge of the network, on the actual sensors of the device. This computing power usually comes in the form of microchips or micro-controllers embedded on the device. For that reason, the processing capability is much more limited as these sensors usually also have to record data from environment and transfer the information recorded to a data storage in the network. Data transfer uses much more battery power than an equivalent computing process. So, by having computing power on the sensor, the data can be processed, preconditioned, and optimized first before being stored. The resulting data will be much smaller, consuming less power in the transfer (27). Mist computing is a great fit for low power situations where extending battery life is a core concern.

**Mist computing allows for the following features:**

- Local analytics and decision-making data.
- Highly robust data and applications.

***Cite this article as:*** *Subbanna, S., & Ganesan, S. (2020). CLOUD COMPUTING IN INTERNET OF THINGS AND NEED FOR SECURITY. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-31). London, GB: ASDF International.*

- Data access control mechanisms to enforce privacy consent at a local level (25).

Although there is not much of a downside to using mist computing, it is much more complex. Not only are the systems used for mist computing usually application specific, but sensors are often heterogeneous, making implementing a solution more complicated. In addition, the processing power available in the mist computing architecture is often limited, which adds even more constraints to any possible solution.

One final aspect of mist computing is security. Using fog or mist computing enhances data security on the system. In these computing architectures, data is processed locally first before being sent to the remote server. This means any sensitive data can be removed or encrypted first, reducing the amount of security threat the system has to deal with (27).

## INDUSTRIAL INTERNET OF THINGS (IIOT)

The history of the IIoT begins with the invention of the programmable logic controller (PLC) by Dick Morley in 1968 (28). His creation, the Modicon, contributed greatly to General Motors' automatic transmission manufacturing capabilities and significantly influenced the future of the automation industry. With hopes of creating an "apparatus for generating and transmitting digital information," American inventor and businessman Theodore G. Paraskevakos was working on the world's first machine to machine (M2M) devices. Morley's PLC and Paraskevakos's M2M were the first steps taken on the long road to today's IIoT. In the 1980's the standardization of Ethernet connectivity laid the groundwork to physically connect machines from different manufacturers and with the introduction of Ethernet people began to explore the concept of a network of smart devices. When these industrial solution vendors first convened, their human machine interface (HMI) and supervisory control and data acquisition (SCADA) solutions were developed with proprietary communication protocols or driver libraries. With a ubiquitous OS and Ethernet backbone in place, more and more industrial devices became connected. Perhaps the most significant IIoT milestone of the early 2000s was the advent and widespread adoption of cloud technologies (29).

IIoT refers to the interrelated, automated use of machines, devices and sensors that run industrial applications. With a strong focus on big data and machine learning, the IIoT enables industries and enterprises to increase efficiency and reliability in their operations, with reduced reliance on human-to-machine interactions. It also enables new business models or revenue sources from useful data that is collected and shared (30). The IIoT is an evolution of a distributed control system (DCS) that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls. IIoT systems are often conceived as a layered modular architecture of digital technology. The device layer refers to the physical components contains CPS, sensors, or machines. The network layer consists of physical network buses, cloud computing and communication protocols that aggregate and transport the data to the service layer, which consists of applications that manipulate and combine data into information that can be displayed on the driver dashboard. The top-most stratum of the stack is the content layer or the user interface (28).

In the mid-2000s, as the consumer world acquired smartphones, the industrial world was getting smaller and more intelligent PLCs and Distributed Control Systems (DCSs). Hybrid controllers and Programmable Automation Controllers (PACs) emerged, and legacy hardware evolved as battery and solar power became more reliable and economical. Manufacturers could power sensors across a distributed architecture, like an oil pipeline, to empower intelligence and connectivity at the farthest reaches of an organization. The combination of widespread power sources and connectivity with smart devices began to add meaningful context to industrial data (29).

In summers 2015 Industrial Internet Consortium (IIC) released the Industrial Internet Reference Architecture (IIRA). The IIC is the largest of the Internet of Things (IoT) consortia with over 170 members (iiconsortium.org) targeted for Industrial Internet. The Industrial Internet Reference Architecture is the product of hundreds of hours of work by the members of the Industrial Internet Consortium Technology Working Group. The first public release of the IIRA is a formal overview of the systems architecture from a high-level perspective: It covers everything from business goals to system inter-operability. The reference architecture explicitly identifies four separate but interrelated sets of concerns and points of view: The business viewpoint, the usage viewpoint, the functional viewpoint, and the implementation viewpoint (31).

For the past few years, systems developers have focused on interconnecting sensors, edge nodes and analytics to build smart systems, transforming operations into significant productivity environments (30).

While the term 'fourth industrial revolution' has been tossed around for a few years, there are various definitions. Coming on the heels of the third industrial revolution, which is also called the digital revolution, the fourth industrial revolution adds new ways for technology and connected devices to be used in business and society. Some of the emerging fields in the fourth industrial revolution include IoT, robotics, machine learning, artificial intelligence (AI), nanotechnology, quantum computing and biotechnology (32). Industrie 4.0 (also known as Industry 4.0) was initiated by the German government as part of its “High-Tech Strategy 2020” in 2010. Industrie 4.0 is all about connected value chains: Industrial industries can connect and automatically integrate things and processes to form cyber physical systems. The ultimate goal of Industrie 4.0 is to increase the value in manufacturing environments and reduce waste through the use of new technologies (30).

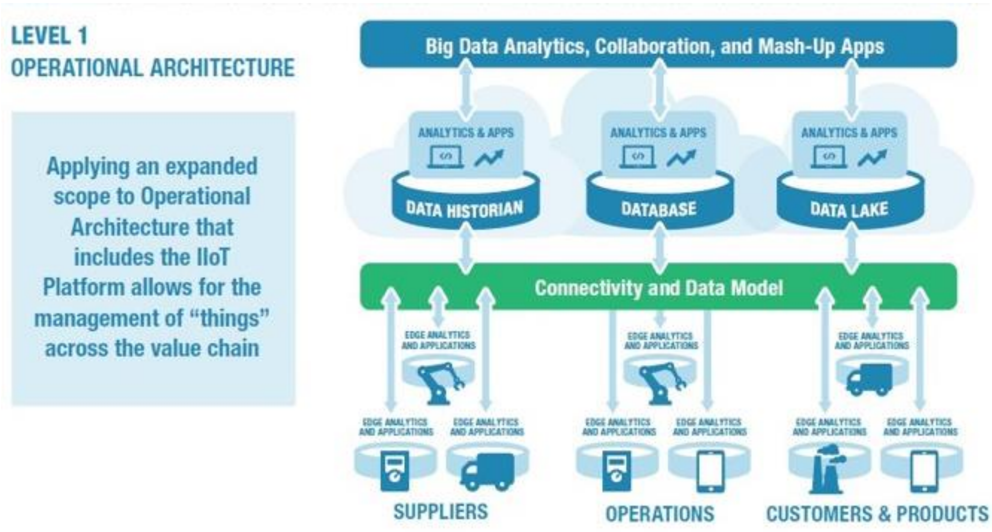

LEVEL 1
OPERATIONAL ARCHITECTURE
Applying an expanded scope to Operational Architecture that includes the IIoT Platform allows for the management of "things" across the value chain
Big Data Analytics, Collaboration, and Mash-Up Apps
ANALYTICS & APPS
ANALYTICS & APPS
ANALYTICS & APPS
DATA HISTORIAN
DATABASE
DATA LAKE
Connectivity and Data Model
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
EDGE ANALYTICS AND APPLICATIONS
SUPPLIERS
OPERATIONS
CUSTOMERS & PRODUCTS

Figure 8: Industrial Internet of Things

Managing IIoT dataflow is critical to ensuring IIoT applications work as designed. A proven architecture put forward by the Industrial Internet Consortium is the databus. In contrast with a database, which manages historical data at rest, the databus manages data in motion. A databus is a data-centric software framework that distributes and manages real-time data in the IIoT, enabling applications and devices to work together as one integrated system. The databus simplifies application and integration logic. Instead of exchanging messages, software components communicate via shared and filtered data objects. Applications directly read and write the value of these data objects, which are cached locally. IIoT streamlines and automates, leading to productivity gains, more efficient operations, cost savings and revenue-generation opportunities. Higher levels of automation and improved product quality, combined with more efficient operations through predictive maintenance, are just some of the ways that IIoT can streamline operations.

Cyberattacks can inflict damage to the systems causing huge financial losses at best and serious injuries or even death at worst. IIoT security is something that must be designed from the ground up, not as an additional protective layer after the system has been built. There are several excellent resources on security, yet it still remains the top concern of IIoT systems. Interoperability is another challenge as connected IIoT system rely on rapid, immediate, and complete accurate data exchange, across systems and across geographic areas. From the sensor to the machine to the enterprise system, data needs to be collected, analyzed, stored, retrieved, and acted upon, seamlessly. Lack of interoperability and lack of standards between IIoT sensors, devices, and applications hinder the communications of IIoT systems (30). Existing cybersecurity measures are vastly inferior for internet-connected devices compared to their traditional computer counterparts, which can allow for them to be hijacked for DDoS-based attacks by botnets like Mirai. Another possibility is the infection of internet-connected industrial controllers, like in the case of Stuxnet, without the need for physical access to the system to spread the worm. Additionally, IIoT-enabled devices can allow for more "traditional" forms of cybercrime, as in the case of the 2013 Target data breach, where information was stolen after hackers gained access to Target's networks via credentials stolen from a third party HVAC vendor (28).

**Industrial IoT capabilities require widespread digitization of manufacturing operations. Organizations must include four primary pillars to be considered a fully IIoT-enabled operation:**

- Smart machines equipped with sensors and software that can track and log data.
- Robust cloud computer systems that can store and process the data.
- Advanced data analytics systems that make sense of and leverage data collected from systems, informing manufacturing improvements and operations.
- Valued employees, who put these insights to work and ensure proper manufacturing function.

**Some of the benefits of Industrial Internet of Things (IIoT)**

- **Increase efficiency**: The biggest benefit of IIoT is that it gives manufacturers the ability to automate, and therefore optimize their operating efficiency.
- **Reduce Errors:** Industrial IoT empowers manufacturers to digitize nearly every part of their business. By reducing manual process and entries, manufacturers are able to reduce the biggest risk associated with manual labor – human error.
- **Predictive Maintenance:** When maintenance in the manufacturing world is reactive rather than proactive, manufacturers are stuck trying to identify what the issue is, how it can be repaired, and what it will cost. With predictive maintenance powered by industrial IoT solutions, all of those issues are alleviated.
- **Improve Safety:** All of the data and sensors required of a fully functioning IIoT manufacturing operation are also helping to bolster workplace safety. "Smart manufacturing" is turning into "smart security" when all of the IIoT sensors work together to monitor workplace and employee safety.
- **Reduce Costs:** Data-driven insights into operations, production, marketing, sales, and more can steer businesses in a profitable direction (33).

Robust industrial connectivity, advanced analytics, condition-based monitoring, predictive maintenance, machine learning, and augmented reality—these are the future of IIoT concepts, backed by viable technology that is available today. Technology leaders—including GE, IBM, PTC, and many more—are thinking on the future of the IIoT in a big way. Over the last years, major investments in innovation and acquisitions have further refined these emerging IIoT platforms. While it is difficult to predict exactly how the IIoT will evolve, it is clear that it is reaching a tipping point in this new industrial revolution. As more devices become connected and more data is created to feed into increasingly powerful analytics and artificial intelligence programs, there is seemingly no limit to the advances that can be made around the IIoT (29).

## CHALLENGES OF INTERNET OF THINGS

The Internet of Things is a universe of connected things providing key physical data and further processing of that data in the cloud to deliver business insights presents a huge opportunity for many players in all businesses and industries. Many companies are organizing themselves to focus on IoT and the connectivity of their future products and services (34). While IoT devices bring effective communication between devices, automate things, saves time and cost, and have numerous benefits, there are few challenges in implementation of IoT that still concerning the manufacturers, enterprises, and users. Several smart TVs and cash machines have been hacked, which is negatively impacting the trust.

- **Outdated hardware and software:**

The increased popularity and usage of IoT has put the manufacturers to focusing on designing and marketing new ones for race in the market that not enough attention is being given to securing the current ones and the legacy devices which are already in use. A majority of these devices do not get enough updates, whereas some of them never get a single one. This implies that the products are secure at the time of purchase but becomes vulnerable to attacks when the hackers find some bugs or security issues. When these issues are not fixed by releasing regular updates for hardware and software, the devices remain vulnerable to attacks. For every little thing connected to the Internet, the regular updates are a must-have. Not having updates can lead to data breach of not only customers but also of the companies that manufacture them.

- **Use of weak and default credentials:**

Many IoT companies are marketing devices with default credentials to access them — like an admin username. Hackers need just the username and password to attack the device. When they know the username, they carry out brute-force attacks to infect the devices.

The Mirai botnet attack is an example that was carried out because the devices required default credentials to access it. The IoT customers are not given instructions from the manufacturers to change the default credentials. Not making an update in the instruction guides leaves all of the devices open to attack (35). The Mirai botnet, used in some of the largest and most disruptive DDoS attacks is perhaps one of the best examples of the issues that come with shipping devices with default passwords and not telling consumers to change them as soon as they receive them. Weak credentials and login details leave nearly all IoT devices in the network vulnerable to password hacking and brute forcing in particular (36). As, the attacked device acts as the gateway to the network which leads to hack all the device in the network.

- **Malware and ransomware:**

The rapid rise in the development of IoT products has made cyberattack permutations unpredictable. Cybercriminals have become advanced today — and they lock out the consumers from using their own device (35). While the traditional ransomware relies on encryption to completely lock out users out of different devices and platforms, there is an ongoing hybridization of both malware and ransomware strains that aims to merge the different types of attack. The ransomware attacks could potentially focus on limiting and/or disabling device functionality and stealing user data at the same time (36). Even top companies like Apple, known for big security claims, and visionaries like Elon Musk have not been spared by hackers. Recent cases of ransomware attacks have also challenged the confidence of corporate (37).

- **Predicting and preventing attacks:**

Cybercriminals are proactively finding out new techniques for security threats. In such a scenario, there is a need for not only finding the vulnerabilities and fixing them as they occur but also learning to predict and prevent new threats. The challenge of security seems to be a long-term challenge for the security of connected devices. Modern cloud services make use of threat intelligence for predicting security issues. Other such techniques include AI-powered monitoring and analytics tools.

- **Difficult to find if a device is affected:**

Although it is not really possible to guarantee 100% security from security threats and breaches, the thing with IoT devices is that most of the users do not get to know if their device is hacked. When there is a large scale of IoT devices, it becomes difficult to monitor all of them even for the service providers. It is because an IoT device needs apps, services, and protocols for communication. Since the number of devices is increasing significantly, the number of things to be managed is increasing even more. Hence, many devices keep on operating without the users knowing that they have been hacked (35). As important as large-scale attacks can be, the IoT industry should be fearing in 2018 are the small-scale attacks that evade out detection. It can be guaranteed that there will be more and more micro-breaches slipping through the security net in the next couple of years. Instead of using the big guns, hackers will most likely be using subtle attack small enough to let the information leak out instead of just grabbing millions and millions of records at once (36).

- **Data protection and security challenges:**

In this interconnected world, the protection of data has become really difficult because it gets transferred between multiple devices within a few seconds. One moment, it is stored in mobile, the next minute it is on the web, and then the cloud. All this data is transferred or transmitted over the internet, which can lead to data leak. Not all the devices through which data is being transmitted or received are secure. Once the data gets leaked, hackers can sell it to other companies that violate the rights for data privacy and security (35). IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even the radio in your car are signifying a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes (34). There has been no research in security vulnerabilities and its improvements. It should ensure Confidentiality, Integrity and Availability of personal data of patient (38). Many people are not aware of IoT, but they understand the dependence on Smart Apps like news apps, stocks applications, entertainment applications. It is not actually important for the consumers to know how things work technically, but lack of basic awareness can create a fear of security and cost, which could lead to the slow adoption of technology (37)

- **Connectivity and data management:**

From data collection and networking point-of-view, the amount of data generated from connected devices will be too high to handle. It will undoubtedly need the use of AI tools and automation. IoT admins and network experts will have to set new rules so that traffic patterns can be detected easily. However, use of such tools will be a little risky because even a slightest of mistakes while configuring can cause an outage (35). Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.This model is sufficient for current IoT ecosystems, where tens, hundreds or even thousands of devices are involved. But when networks grow to join billions and hundreds of billions of devices, centralized systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities. Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker. Networks will be created in meshes with no single point of failure. This model will have its own set of challenges, especially from a security perspective, but these challenges can be met with some of the emerging IoT technologies such as Blockchain (34). This is critical for large enterprises in healthcare, financial services, power, and transportation industries (35).

With the launch of Big Data frameworks such as Hadoop and Cassandra, the problem and complexity of handling unstructured data has somewhat reduced, but the Big Data in itself is so massive that combining it with IoT possess a great challenge. Besides, there are no standard guidelines for retention and use of data as well as metadata (37). Structured data are stored in relational databases and queried through SQL for example. Unstructured data are stored in different types of NoSQL databases without a standard querying approach. Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems. Artificial intelligence models can be improved with large data sets that are more readily available than ever before, thanks to the lower storage (34).

- **Home security:**

Today, more and more homes and offices are getting smart with IoT connectivity. The big builders and developers are powering the apartments and the entire building with IoT devices. While home automation is a good thing, but not everyone is aware of the best practices that should be taken care of for IoT security. Perhaps one of the scariest threats that IoT can possess is of the home invasion. Even if the IP addresses get exposed, this can lead to exposure of residential address and other contact details of the consumer. Attackers or interested parties can use this information for evil purposes. This leaves smart homes at potential risk.

- **Security of autonomous vehicles:**

Just like homes, the self-driving vehicles or the ones that make use of IoT services, are also at risk. Smart vehicles can be hijacked by skilled hackers from remote locations. Once they get access, they can control the car, which can be very risky for passengers. Undoubtedly, IoT is a technology that should be called a boon. But since it connects all the things to the Internet, the things become vulnerable to some sort of security threats. Big companies and cybersecurity researchers are giving their best to make things perfect for the consumers, but there is still a lot to be done (35). Smart cars are on the verge of becoming reality with the help of connected IoT devices. However, due its IoT association, it also possesses a greater risk of a car hijack. A skilled hacker might hijack by getting the access of your smart car through the remote access. This will be scary situation as anyone can have control over your car and it can leave you vulnerable to lethal crimes (36).

## BIBLIOGRAPHY

1. **researchgate.** Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. [Online] May 2016. https://www.researchgate.net/publication/330425585.

2. **Keith D. Foote.** A Brief History of the Internet of Things. [Online] August 16, 2016. https://www.dataversity.net/brief-history-internet-things/#.

3. **CISCO.** The Internet of Things. *How the next evolution of IoT is changing everything.* [Online] April 2011. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

4. **Texas Instruments.** The Evolution of the. [Online] September 2013. https://www.ti.com/lit/ml/swrb028/swrb028.pdf?ts=1590511408949.

5. **Paul Strokes.** 4 Stages of IoT architecture explained in simple words. [Online] April 2011. https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f.

6. **Adam Calihman.** Architectures in the IoT Civilization. *Netburner.* [Online] January 30, 2019. https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/#:~:text=There%20are%20essentially%20three%20major,interoperability%20are%20major%20driving%20factors..

7. **Pallavi Sethi and Smruti R. Sarangi.** Internet of Things: Architectures, Protocols, and Applications. *Journals of Electrical and Computer Engineering.* [Online] Hindawi, Jan 26, 2017. https://www.hindawi.com/journals/jece/2017/9324035/.

8. **Rouse, Margaret.** Cloud Computing. [Online] https://searchcloudcomputing.techtarget.com/definition/cloud-computing.

9. **Wikipedia.** Cloud computing. [Online] June 22, 2020. https://en.wikipedia.org/wiki/Cloud_computing#:~:text=Cloud%20computing%20is%20the%20on,many%20users%20over%20the%20Internet..

10. **Microsoft Azure.** Whatis cloud computing? [Online] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/.

11. **Steve Ranger .** What is cloud computing? Everything you need to know about the cloud explained. [Online] ZDNet, December 13, 2018. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/.

12. **Wikipedia.** Fog computing. *Wikipedia.* [Online] June 26, 2020. https://en.wikipedia.org/wiki/Fog_computing.

13. **Joe McKendrick .** Fog Computing: a New IoT Architecture? *RTInsights.* [Online] March 22, 2016. https://www.rtinsights.com/what-is-fog-computing-open-consortium/.

14. **Rick Blaisdell.** IoT and the Fog Computing Architecture. *Rick's Cloud.* [Online] April 27, 2017. https://rickscloud.com/iot-and-the-foggy-architecture/.

15. **Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli.** Fog Computing and Its Role in the Internet of Things. [Online] August 17, 2012. https://dl.acm.org/doi/pdf/10.1145/2342509.2342513.

16. **Seung Woo Kum, Jaewon Moon, Tae-Beom Lim.** Design of Fog Computing based. [Online] Septemer 2017. https://ieeexplore-ieee-org.huaryu.kl.oakland.edu/stamp/stamp.jsp?tp=&arnumber=8210598&tag=1.

17. **IEEE Innovation.** Edge Computing Resources. [Online] https://innovationatwork.ieee.org/edge_computing/.

18. **B.Panchali.** Edge Computing- Background and Overview. [Online] April 2018. https://ieeexplore-ieee-org.huaryu.kl.oakland.edu/stamp/stamp.jsp?tp=&arnumber=8748352&tag=1.

19. **Wikipedia.** Edge computing. *Wikipedia.* [Online] June 29, 2020. https://en.wikipedia.org/wiki/Edge_computing.

20. **Keith Shaw.** What is edge computing and why it matters. [Online] Nov 13, 2019. https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html.

21. **Ashok Iyengar.** Architecting at the Edge. [Online] Oct 21, 2019. https://www.ibm.com/cloud/blog/architecting-at-the-edge.

22. **IEEE.** Why Does Edge Computing Matter? *IEEE Innovation at work.* [Online] IEEE. https://innovationatwork.ieee.org/why-does-edge-computing-matter/.

23. **YuanAi, MugenPeng & KechengZhang.** Digital Communications and Networks. *Science Direct.* [Online] April 2018. https://www.sciencedirect.com/science/article/pii/S2352864817301335.

24. **Radiocrafts.** Cloud vs Fog vs Mist Computing, Which One Should You Use? [Online] April 30, 2019. https://radiocrafts.com/cloud-vs-fog-vs-mist-computing-which-one-should-you-use/#:~:text=Mist%20Computing,centralised%20(cloud)%20computing%20services.

25. **Thinnect.** Evolution of Mist Computing from Fog and Cloud Computing. [Online] https://www.thinnect.com/static/2016/08/cloud-fog-mist-computing-062216.pdf.

26. **Rabindra K. Barik, Amaresh Chandra Dubey, Ankita Tripathi, Tanjappa Pratik, Sapana Sasane, Rakesh Kumar Lenka, Harishchandra Dubey, Kunal Mankodiya & Vinay Kumar.** Mist Data: Leveraging Mist Computing for Secure and Scalable Architecture for Smart and Connected Health. *Research Gate.* [Online] 2017. https://www.researchgate.net/publication/322350973_Mist_Data_Leveraging_Mist_Computing_for_Secure_and_Scalable_Architecture_for_Smart_and_Connected_Health.

27. **Mahesa, Raka.** How cloud, fog, and mist computing can work together. *IBM.* [Online] Mar 06, 2018. https://developer.ibm.com/technologies/iot/articles/how-cloud-fog-and-mist-computing-can-work-together/.

28. **Wikipeadia.** Industrial internet of things. [Online] May 20, 2020. https://en.wikipedia.org/wiki/Industrial_internet_of_things#:~:text=The%20current%20conception%20of%20the,devices%2C%20programs%2C%20and%20data%20sources.

29. **Paine, Tony.** Our (info)graphic, short history of the Industrial Internet of Things. *readwrite.* [Online] Dec 05, 2016. https://readwrite.com/2016/12/05/history-industrial-internet-of-things-il4/.

30. **Lynne Canavan.** What is IIoT? The Industrial Internet of Things Primer. [Online] RTI, Sept 4, 2019. https://www.rti.com/blog/the-iiot-primer.

31. **Tomi Engdahl.** Industrial Internet Reference Architecture. [Online] ePanorama, Sept 25, 2015. https://www.epanorama.net/blog/2015/09/25/industrial-internet-reference-architecture/.

32. **Teena Maddox .** How IoT will drive the fourth industrial revolution. [Online] ZDet, March 1, 2019. https://www.zdnet.com/article/how-iot-will-drive-the-fourth-industrial-revolution/.

33. **Michael Mendoza.** Industrial IoT - The Top 5 Benefits of Industry 4.0. [Online] HItachi Solutions. https://global.hitachi-solutions.com/blog/industrial-iot-benefits.

34. **Ahmed Banafa.** Three Major Challenges Facing IoT. *IEEE Interrnet of Thngs.* [Online] March 2017. https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html.

35. **Vaibhav Shah .** 9 Main Security Challenges for the Future of the Internet Of Things (IoT). *readwrite.* [Online] Sept 05, 2019. https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/.

36. **Angelina Harper.** 10 Biggest security challenges for IoT. *Peerbits.* [Online] https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

37. **Rita Sharma.** Top 10 Challenges Enterprises Face In IoT Implementation. *Finoit.* [Online] https://www.finoit.com/blog/enterprise-challenges-in-iot/.

38. **Kothari, Jash.** Challenges in World Of IoT. *GeeksforGeeks.* [Online] https://www.geeksforgeeks.org/challenges-in-world-of-iot/.

39. **GSMA.** Understanding the. [Online] July 2914. https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf.

40. **Smart Card Alliance.** Embedded Hardware Security for. [Online] December 2016. https://www.securetechalliance.org/wp-content/uploads/Embedded-HW-Security-for-IoT-WP-FINAL-December-2016.pdf.

41. **P.P Ray.** A Survey on IoT architectures. [Online] July 2018. https://www.sciencedirect.com/science/article/pii/S1319157816300799.

42. **Kounte, Soumyalatha Naveen & Manjunath R.** Key Technologies and challenges in IoT Edge. [Online] January 2019. https://ieeexplore-ieee-org.huaryu.kl.oakland.edu/stamp/stamp.jsp?tp=&arnumber=9032541.

43. **Cloudflare.** What Is Edge Computing? *Cloudflare.* [Online] 2020. https://www.cloudflare.com/learning/serverless/glossary/what-is-edge-computing/.

| | |
|---|---|
| ISBN | 978-93-88122-13-9 |
| Website | www.iccotwt.com |
| Received | 24 June 2020 |
| Article ID | iccotwt.2656 |

| | |
|---|---|
| VOL | 01 |
| eMail | iccotwt@asdf.res.in |
| Accepted | 01 July 2020 |
| eAID | 2020.iccotwt.2656 |

# ROLE OF CONTEXT-AWARE SYSTEM IN SMART HEALTHCARE ENVIRONMENTS: A TECHNICAL STUDY

**Manimurugan S[1], Narmatha C[1], Rajmohan R[2], and Rajendran T[2]**

[1]*Faculty of Computers and Information Technology, University of Tabuk, Kingdom of Saudi Arabia.*

[2]*Makeit Technologies (Center for Industrial Research), Coimbatore, India.*

**ABSTRACT:** In the present world, mobile computing devices are popular and are identified in each aspect of life. This combination of computing and the present world is not restricted to everyday life. The medical field was similarly concerned, where care is given in a wide scope of areas and conditions. Therefore, two aspects are considered to the combination of computing and the healthcare frameworks, called m-health and e-health. E-health could be described as any electronic sharing of healthcare-associated data over organizations. However, the more specific part of e-health called mobile health, or m-health was health care simpler by the combination of mobile and desktop health care with mobile wireless technology. M-health has emerged global utilization with its high range and minimal cost arrangements. The medical domain is continually being immersed with new kinds of innovations, including context-aware systems and applications. This paper was proposed to review the context-aware system, context-aware models, and context-aware system in health care applications.

**Key Words:** Context-aware system, smart healthcare, sensors, IoT, Cloud

***Cite this article as:*** *S, M., C, N., R, R., & T, R. (2020). ROLE OF CONTEXT-AWARE SYSTEM IN SMART HEALTHCARE ENVIRONMENTS: A TECHNICAL STUDY. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-10). London, GB: ASDF International.*

## I. INTRODUCTION

With the quick advancement of mobile communication innovation and UI innovation, numerous mobile internet devices, for example, PDA, laptop, notebook, smartphone, and so on, have been exceedingly considered by current society. Ubiquitous computing is turning into a reality that highlights the integration between the data space and the physical space. With its assistance, individuals could receive and process data whenever and anyplace through a device that can link any internet. Therefore, it can lessen the difficulty of utilizing the device and make individuals' lives simpler and progressively effective. The environment of users in ubiquitous computing, for example, the location, or terminal equipment, and so on, is continually changing, which is called context. As part of the central zones of ubiquitous computing, context-aware computing has become increasingly very well known among people [1].

Numerous authors have described context according to their comprehension with an exertion to review a great basic idea of the context [2]. Schilit and Theimer utilized the label context-aware in 1994 and depicted as location, similarities, objects, and close by individuals. In 1996 Brown described context as the components which encompass the user, which the system could detect. A regularly referred to and very conventional meaning of context was that by Dey and Abowd: Context is any data that could be utilized to describe the circumstance of the entity. An entity is an individual, object, or place which is viewed as important to the collaboration among the user and the applications, comprising the client and application themselves" [3]. The context was valuable, and individuals have functioned on it, concentrating on the area for the most part, even though the circumstance of an entity may comprise of location, time, activity, and the encompassing conditions that may influence the action of the entity.

The label context has been sorted into two classes (logical and physical) [4]. The physical context could be decided through a hardware sensor, and logical context was either provided through the user's feedback or by observing their communications with the services accessible, for instance, by monitoring or reviewing the user's profile, working schedules, activities, composing movement, and so on. Most research around there utilizes physical sensors for movement, sound, touch, temperature, light, and of course, location. The logical sensor, though, gives associated data by reading user's data from public website pages and different archives and reviews user's information (interaction) and dependent on those interaction target publicizing [2].

## II. CONTEXT AND CONTEXT AWARE SYSTEMS

### a. Context Properties

A presented context was made of various elements, out of which we can simply distinguish:

- Location: Position, direction, speed, and so forth.
- User Identity: Profile, inclinations, biometrics, social data, and so forth.
- Time: Present date and time or future occasions, duration, and so forth.
- Activity: Walking, resting, sitting, and so forth.
- Current Task: Work or social gathering, wellness, studying, and so forth.
- Environment: Temperature, humidity, light, and noise levels.
- Hardware: Present device data, network, and encompassing devices [5].

Context-awareness refers that one can utilize context data. A system was context-aware if that it could extricate, decrypt, and use context data and modify their performance to the present context of usage. The name context-aware computing was generally perceived through those performing in context-aware, where it was considered that context was a source in its attempt to distribute and directly combine computer advancement into our lives [6].

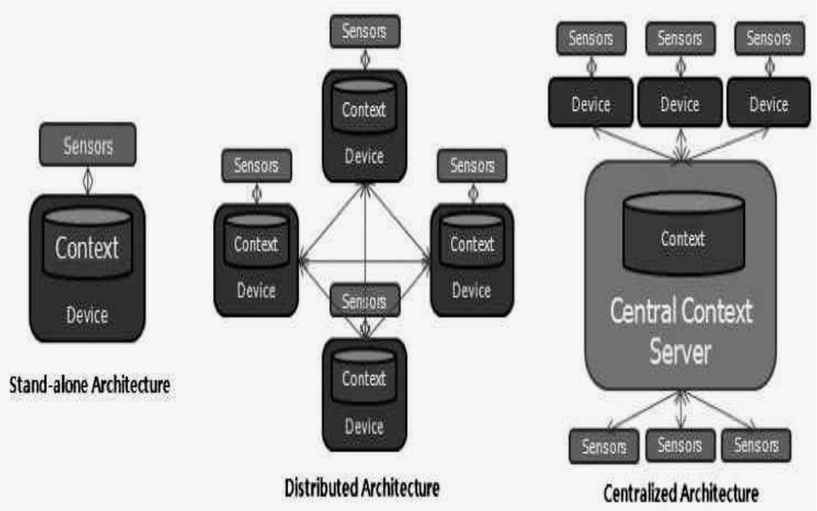


Figure.1. Context-Aware Architecture Types

Stand-alone Architecture, which is an essential architecture that specifically gets to the sensor, does not consider device context sharing. This architecture could generally be effortlessly actualized however have confinements because of how it could not operate device coordinated effort. This architecture is suitable for less, basic, or domain explicit applications.

Distributed Architecture Context-aware frameworks, which have distributed architecture, could store context data in a lot of isolated devices, and there is no other central server. Every device is free of different devices. Therefore, the CAS could overlook some less vital devices that have blockage issues and still proceed through tasks of context-aware. Every device deals with their context data and offers context data with different devices by communicating through different devices. Thus, ad-hoc communication conventions are required. In any case, it is difficult for devices to know the general circumstance of each device while utilizing ad-hoc communication conventions. Normally, cell phones need computation control and resources; also, a distributed architecture is among confinements in managing computationally serious applications.

Centralized Architecture (Context Server) devices and sensors are associated with a centralized context server that has rich resources and computational control, and context data can be saved in both a central server and user devices. If a device must get context data of other devices, the device demands the focal server and gets the outcome. In this architecture, each transmission is executed by requesting the context server so that the transmission protocol could be moderately basic than distributed design. By utilizing a computationally incredible device as a central server, numerous applications which require great resources and cost could be handled. Notwithstanding, there is an inconvenience of this methodology that it tends to be critical if the central server fails or congestion happens[7].

Context-aware systems (CAS) can modify their activities dependent on the present context. This likewise expands adequacy by considering the environmental context. CAS observes the condition constantly and proposes reasonable recommendations to users in which they could make important actions, i.e., distributing the user's place to suitable individuals from the social network, and enabling dealers to distribute exceptional offers to essential clients who are close to the traders.CAS utilized an assortment of contexts like location, condition, and device. The user's present place to a device was treated as a context. An environmental context comprises the circumstances of an environment. The system modeling device context incorporates changing display intensity dependent on the available battery power. User contexts incorporate their physical activity, the method of transport and activity logs of a user, utilization types for transport and procurement references, and so on [8].

In CAS, the context could be raw information and important data utilized to extract choices. Information could emerge from different sources. For characterizing context, the information should be preprocessed. At the point when the information is different, it must be standardized and aggregated[2].

## III. CONTEXT-AWARENESS MODELS

CAS could be utilized in several conditions. The typical method considers various special prerequisites and circumstances, for example, the sensors location (local or far away), number of potential users, accessible resources (for example, top quality PCs or cell phones), and expandability of the system. Applications of context-aware are commonly dependent on Context-Aware models. Strang and LinnhoffPopien described the most applicable context-modeling schemes dependent on data structure utilized for presenting and sharing contextual data in their system(Komal T and Amit B, 2015). The context modeling schemes are,

**Key-value model:** It represents the basic data structures for context modeling. They are constantly utilized in different service systems, where key-value sets were utilized to represent the abilities of service. Service discovery is then implemented with suitable algorithms that utilize these key-value sets.

**User context perception models:** It is made to enable the developer to comprehend the difficulties faced in making CAS. For instance, a car GPS performs well indeed if one is in a new location; but once utilizing it somewhere a popular place, one could eventually be surprized at the route it attempts for guiding one as well.

***Mark-up model:*** This utilizes hierarchical data structures, including mark-up labels, properties, and contents, to make a profile that represents the common mark-up model.

**Graphical model:** Many techniques have been presented where contextual perspectives were modeled utilizing Unified Modeling Language.

**Object-oriented model:** Modeling context utilizing this method provides the total power of object orientations (for example, reusability, encapsulation, and succession). Present techniques utilize different items to describe various context data, (for example, location, temperature, and so on.) and encapsulate information of context process and presentation. Access to the context and context-processing logic was given through well-characterized associations such as the hydrogen model.

**Logic-based model:** This model has a high level of convention, and common facts, conditions, and standards are utilized to describe the context model. The logic-based framework was utilized to deal with the previously mentioned conditions and permits inclusion, upgrading, or removing new factual data. The inference (additionally named reasoning) process was utilized to determine new factual data dependent on existing standards in the system. Contextual data was hence depicting a proper manner as factual data.

**Ontology-based model:** It describes the representation of ideas and their relations. This model is successful for modeling contextual data because of its high and proper expressiveness and eventualities for implementing ontology reasoning methods [4].

## IV. DISCUSSION

### a. Context-Aware in Healthcare

The combination of computer science and the medical domain is a progressive innovation, with present research aiming at the use of computing to support in training among the medical sector. The smart clinical devices market was predicted to reach $25 billion profit by the year 2025, while smart connected wearable gadgets intended to be extensively utilized to accomplish enhanced health, quality of life, and protection of citizens. Moreover, to their capability to aid real-time constant observance of patient's vital signs, such devices also make context-aware mobility significant to enhance the overall condition of medical care [10]. CAS is a system that can adjust their activities to context changes without unequivocal user intercession. The CAS platform should unequivocally present by its component's functionalities, context data, and the control activity and provides services to clients utilizing context data where pertinence relies upon the client's operation. In this way, a context-aware domain could be intended middleware support that permits the exchange of environmental data out of the minimum infrastructure range to a more significant range for definition and decision. This multi-layered design was common for the Cloud computing sequence that permits setting the middleware layer as a major aspect of a Sensor-Cloud interface in the layer of PaaS (Platform as a Service) [11].

From the most recent decade, the CAS targets web applications and desktop computing to the Internet of Things (IoT). Because of advanced sensor innovation, sensors are getting stronger, less expensive, and minimum in size. In this present world, we have many sensors, and eventually, this sensor creates a lot of information, for example, big data. Except if we dissect, interpret, and comprehend the information collected, that information may not produce important data. Context-aware computing plays a significant part in handling this task, for example, mobile and pervasive, which would be effective in the IoT model also. This enables us to save the context data associated with sensor information, so the interpretation should be possible all the more effectively, genuinely, and the context makes it simpler to execute machine-to-machine interaction as it is the core component in the IoT condition [12].

In the present world, Context information has been proved to enhance the user's experience in mobile apps. Some of the health care applications based on a context-aware system has been analyzed and discussed below.

TABLE.1. REVIEW ON DIFFERENT HEALTHCARE APPLICATIONS BASED ON CONTEXT-AWARE SYSTEM

| Author | Year | Title | Application |
|---|---|---|---|
| **Shankari B et al. [13]** | 2011 | Context-Aware Health Care Application | It was reporting crucial health issues of a patient who was suffering from brain tumors based on the ontology model. |
| **I-Ching Hsu [20]** | 2013 | Wireless Context-Aware Healthcare System Based on sensor Web 2.0 | RFID-based Context-aware Healthcare System (RCHS) that was depended on the architecture of wireless communication and was used in the Web 2.0 condition. The RCHS was comprised of RFID-based Healthcare sensors, RFID-based, Context-aware Healthcare Middleware, and Mobile user to permit a constant and context-aware health observance for patients. |

| | | | |
|---|---|---|---|
| **F. Paganelli and D. Giuli [12]** | 2013 | An Ontology-based System for Context-aware and Configurable Services to Support Home-based Continuous Care | Ontology-based context modeling and the associated context management model was presenting a configurable and extendable service-adapted system to simplify the improvement of applications for observing and analyzing chronic patient conditions. |
| **Abishek T K [19]** | 2013 | WiCard: A Context-Aware Wearable Wireless Sensor for Cardiac Monitoring | To monitor and assist the patients with Cardiovascular disease based on the Wearable Wireless Cardiac Monitoring (WiCard) system. This context-aware model is used to relate the physical activity and Physiological signals of the user. |
| **Albert Pla et al. [14]** | 2015 | Context Management in Health Care Apps | Smart e-Health monitoring application for remote patients. Specifically, the app was intended for aiding parents responsible for prematurely born kids through a mobile phone application and a group of sensors. |
| **Yvette E. G. et al. [15]** | 2015 | Context-Aware Computing for Delivering u-Healthcare Services | CAS for the u-healthcare system depended on component-based improvement. By use of the sensor interface model and multi-purpose gateway to handle the contextual information and forward to clinics, hospitals, or patients mobile as u-healthcare services. |
| **Nirmalya R et al. [18]** | 2016 | Quality and Context-Aware Smart Health Care | A remote context monitoring in a smart assisted living environment for an aged individual. The smart home might be set with various sensors [light, humidity, ECG, EMG, etc.] |

***Cite this article as:*** *S, M., C, N., R, R., & T, R. (2020). ROLE OF CONTEXT-AWARE SYSTEM IN SMART HEALTHCARE ENVIRONMENTS: A TECHNICAL STUDY. In Proceedings of International Conference on Cloud of Things and Wearable Technologies 2020. (6th ed., Vol. 1, pp. 01-10). London, GB: ASDF International.*

| | | | |
|---|---|---|---|
| **Richard A.W.T and Kinshuk [9]** | 2017 | A mobile context-aware medical training system for the reduction of pathogen transmission | An effort to minimize the causalities due to pathogen transmissions in hospitals. |
| **Mirza Muhammad B.B and Muhammad T.J [11]** | 2017 | An iBeacon based Real-time Context-Aware e-Healthcare System | Real-time context-aware health care services to older patients. The proposed solution was context-aware by identifying health status and tracking patients in a real-time order from wearable sensors and iBeacons. |
| **Chimdessa A and Shilpa G [17]** | 2017 | IoT Based HealthCare Remote Monitoring and Context-aware Appointment System | Observe remote patient's health with the advantages of wearable sensors monitor HR, ECG, Temperature, BP, and establish follow up appointment reminder system depended on patient's parameters captured values. |
| **Kathleen Yin et al. [16]** | 2019 | Context-Aware Systems for Chronic Disease Patients: Scoping Review | CAS in enhancing patient work, self-management practices, and health results in chronic disease patients. |
| **Muhammad Ajmal A et al. [10]** | 2019 | A privacy-preserving framework for smart context-aware healthcare applications | Privacy preservation within Electronic Transfer of Prescription. |

## V. CONCLUSION

Context-aware systems (CAS) are a successful method to deal with everyday life activities. Context-aware frameworks present new possibilities for developers of application and end users altogether through collecting context information and adjusting system conduct appropriately. In this paper, we have reviewed the ideology of context awareness and its models and presented a short overview of context-awareness in healthcare. Different models based on context-awareness in healthcare and medical applications were analyzed and discussed. Context-awareness in medical service is an emerging field with the progressive development of new applications on the medical field that have been proposed all over the world. The use of context-awareness in the medical field is embedded with other domains like IoT, Cloud computing, etc. With the combination of integrating with these technologies, the developed application on the context-awareness system has many advantages over other methods. Different applications like health monitoring, analyzing diseases, and assisting on medications can be done remotely with the combinations of these technologies.

## REFERENCES

1. Wei Liu, Xue Li, and Daoli Huang, 2011, A Survey on Context Awareness, International Conference on Computer Science and Service System (CSSS), IEEE, pp.144-147.

2. Pooja S. Gandodhar and S.M. Chaware, 2018, Context Aware Computing Systems: A survey, Proceedings of the Second International conference on I-SMAC, IEEE, pp.605-608.

3. SagarSukode, ShilpaGite, and HimanshuAgrawal, 2015, Context Aware Framework in IoT: A Survey, International Journal of Advanced Trends in Computer Science and Engineering, Volume 4, No.1, pp.1-9.

4. KomalTayde and AmitBhala, 2015, Context Awareness in Mobile Computing, International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 7, pp.112-124.

5. hristos B. Anagnostopoulos, AthanasiosTsounis and StathesHadjiefthymiades, 2006, Context Awareness in Mobile Computing Environments, Wireless Personal Communications (2007), Springer, 42:pp.445–464.

6. George W. Musumba and Henry O. Nyongesa, 2013, Context awareness in mobile computing: A review, Int J Machine Learn Appl, 2(1).

7. RaduDobrescu, Daniel Merezeanu, and Stefan Mocanu, 2019, Context-aware control and monitoring system with IoT and cloud support, Computers and Electronics in Agriculture, Elsevier, Vol.160, pp.91-99.

8. OzgurYurur et al., 2014, Context-Awareness for Mobile Sensing: A Survey and Future Directions, IEEE, pp.1-28.

9. Richard A.W.T and Kinshuk, 2017, A mobile context-aware medical training system for the reduction of pathogen transmission, Smart Learning Environments, Springer, Vol.4, No.4, pp.1-13.

10. Muhammad Ajmal A, Junaid A, Shazia M, Khaled S, and Muhammad Imran, 2019, A privacy-preserving framework for smart context-aware healthcare applications, Trans Emerging Tel Tech, pp.1-20.

11. Mirza Muhammad B.B and Muhammad Taha J, 2017, AniBeacon based Real-time Context-Aware e-Healthcare System, IEEE, pp.1-5.

12. Paganelli F and Giuli D, 2013, An Ontology-based system for Context-aware and Configurable Services to Support Home-based Continuous Care, IEEE, pp.1-10.

13. Shankari B, Saravanaguru RA.K, and Arunkumar T, 2011, Context Aware Health Care Application, International Journal of Advancements in Technology, Vol.2, No.2, pp.461-470.

14. Albert Pla, Beatriz López, Natalia M, Cristina A, and Abel López B, 2015, Context Management in Health Care Apps, International Conference on Autonomous Agents and Multiagent Systems, Vol.4, No.8, pp.1-8.

15. Yvette E. Gelogo, Haeng-Kon Kim, and Rhan Jung, 2015, Context-Aware Computing for Delivering u-Healthcare Services, International Journal of Smart Home, Vol. 9, No. 8, pp. 169-178.

16. Kathleen Yin et al., 2019, Context-Aware Systems for Chronic Disease Patients: Scoping Review, Journal of Medical Internet Research, Vol.21, No.6, pp.1-8.

17. ChimdessaAssaba and ShilpaGite, 2017, IOT Based HealthCare Remote Monitoring and Context-aware Appointment System, International Journal of Current Engineering and Technology, Vol.7, No.6, pp.1-5.

18. Nirmalya Roy, Christine Julien, ArchanMisra, and Sajal K. Das, 2016, Quality and Context-Aware Smart Health Care, IEEE Systems, Man, & Cybernetics Magazine, pp.15-25.

19. Abishek T K, Dilraj N, Manesh M, and Maneesha V R, 2013, WiCard: A Context Aware Wearable Wireless Sensor for Cardiac Monitoring, IEEE, pp.1097-1102.

20. I-Ching Hsu, 2013, Wireless Context-Aware Healthcare System Based on Sensor Web 2.0, International Journal of Innovation, Management and Technology, Vol.4, No.4, pp.414-418.

21. BachirChihani, Emmanuel Bertin, Fabrice Jeanne, Noel Crespi, 2011, Context-aware systems: a case study, The International Conference on Digital Information and Communication Technology and its Applications, Springer, pp.718-732.

22. UnaiAlegre, Juan Carlos Augusto and Tony Clark, 2016, Engineering Context-Aware Systems and Applications: A survey, Journal of Systems and Software, Elsevier, Vol.117, pp.55-83.