International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering 2015 [ICIREIE 2015]

| | | | |
|---|---|---|---|
| **ISBN** | 978-81-929866-3-0 | **VOL** | 01 |
| **Website** | www.icireie.org | **eMail** | icireie@asdf.res.in |
| **Received** | 10 - July - 2015 | **Accepted** | 31- July - 2015 |
| **Article ID** | ICIREIE006 | **eAID** | ICIREIE.2015.006 |


# Enhancing Performance and security for 'Data in Motion ' in BIG DATA

Sarafudheen M Tharayil[1], K.Kalaiselvi[2], Dr. Paul Rodrigues[3], Dr. Anand Kumar[4]

[1]*Research Scholar, Bharathiar University.* Senior IT Architect (BI/ERP), Saudi Aramco, Dhahran, Saudi Arabia.

[2]*Research Scholar, Bharathiar University,* Asst. Professor, Dept of Computer Science, Kristu Jayanti College, Bangalore.

[3]*Research Supervisor, Bharathiar University,* Principal, DMI Engg. College, Palanchur, Chennai, TN.

[4]*Research Supervisor, BU,* Professor & Dean, Dept of CS & Engg., M.S Engg. College, Visvesvaraya Technological University.

***Abstract:*** *As the big data systems increases its size from Terra bytes to Peta and Zeta bytes with its structured, semi-structured and unstructured characteristics; securing the data in its storage and motion is the highest priority in business now. As security is rather a novice topic in big data business, organization such as NIST is currently working on standardizing the architecture framework for Big Data Security. This paper discuss the need, challenges and solutions for the security and privacy of data in motion in a big data security framework. Standard network protocols like Kerberos, SSL, TLS and Big Data specific protocols such as Hadoop RPC and HDFS can be collaborated with secured motion of big data. This paper initiates a collaborated mechanism by using AES cryptographic algorithm with its variants to transfer the big data contents. This paper focus on AES cryptography scheme and how to tune this scheme for better performance for achieving great result in Big Data scenarios. Focusing on the efficiency and performance factors, a Five Steps structure is proposed here that can be adopted in big data systems such as Hadoop.*

***Keywords:*** Hadoop; SAP HANA; Big Data; Data in Motion; Data at Rest; Cryptography ;Symmetric encryption; AES;AES-NI;Security Framework; Advanced Encryption Standard

## I. INTRODUCTION

### A. Big Data and Security-A Hadoop Approach

In distributed Big Data environment, processing of data happens upon availability of resources in a parallel processing heterogeneous environment. Data is sliced into fragments in different servers. Big Data system nodes communicate and execute its application programs across systems using communication protocols and remote calls on TCP/IP. Most cloud based Big Data implementations uses web based user interfaces and need access control at the schema level and most times granular level in heterogeneous and complex systems[13].

Mandated by industry requirements, different Big Data architecture brings unique security challenges. Distributed, scalable and redundant implementations such as Hadoop File System (HDFS) bring unique challenges because it is totally different from conventional systems such as RDBMS database systems [13]. In the past, due to its insecure nature, a malicious user could easily get into a Hadoop node and get access to its file system data hacking the block ID and thus deploying a secure Big Data system was almost impossible. Authentication, authorization, keeping privacy & Personally Identifiable Information (PII), file permission, application program security



**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

and security of data in transit were all weak in Big Data system implementations [5]. Application program code could randomly travel across network and can be submitted as a job in Big Data system [11].

### B. Data Privacy

Major challenge in PII is managing user details, payment details, family data and many other private data. Various standards such as Payment Card Industry Standard(PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and government mandates to follow information security standards enforces to use security mechanism to protect the big data while it is at rest and at motion[13][14][15]. Big Data systems such as Hadoop are still maturing on its security architecture and credibility across organization to achieve the privacy of data. In order to comply with standards and organizational security policies, different security layers are required such as done using Kerberos, Apache Knox, and Apache Rhino in a Big Data lake [11]. Sensitive data within Big Data needs special kind of protection and should be secured both at rest and in motion [10].

### C. Big Data Security Challenges and Limitations

Security challenges such as unauthorized access, unauthorized modification of data and denial of service are still a challenge to Big Data industry. Tasks such as Identifying sensitive information, determining the volume of data at risk, limiting the search facilities, securing the data during transmission, establishing security surveillance, governance mechanism and security scanning tools are very important in Big Data environment these days [1][13]. As of today the authorization model in Hadoop is fragmented and manual. Data by default is unprotected and there is a lack of central authentication and authorization component [2].

### D. Security of Data in Motion (Data in Transit)

The term "Data in motion" is mostly used in association with privacy of data while it is transmitted from one place to another place. Sometimes this term is used in association with the term "Data in Use" where moving the data from storage to the system processor and volatile memory is also sometimes considered as moving data, especially in Big Data scenario where the processing and other computing resources are distributed.

Protecting data while it is moving is important in Big Data systems. The Data in motion is not limited to transfer of data and other information between system nodes, but also it includes the moving data among sensors and smart devices. The volume of Data in motion is increasing rapidly. For instance, statistics shows google system has a volume of five Exabyte of information flowing in their systems which include structured, semi-structured and unstructured data. Industries like Healthcare, retail, supply chain, energy production and network intelligence brings unique requirements and standards for securing data in motion [17].

Hadoop solutions today uses simple authentication and security layer (SASL) for authentication and encryption of data in Motion with built in authentication mechanisms using DIGEST-MD5 and CRAM-MD5. Hadoop supports network security protocols such as secure RPC, HTTPS, SSL, and TLS for securing data in motion with its encryption and masking techniques. Intel distribution offers encryption and compression of files [15]. Project Rhino enables block-level encryption. [5]

### E. Performance and Framework Component of Data in Motion

The performance of encryption techniques for the moving data in Big Data scenario depends not only on the speed of algorithm and the throughput, but on different framework components of the environment and systems. Government legal framework, guidelines adopted by organizations, intellectual property contracts, the hardware and software vendor selection, auditing and monitoring all have an impact on the security mechanism and performance of encryption schemes [18].

## II. Existing Solutions

### F. Overall Big Data Security and Frameworks

Most of the existing Big Data solution can be visualized as shown in the *figure 1* including Hadoop. At the top level, data management involves data classification & prioritization, data discovery and data tagging. As of today, for user validation, identity and role management (RBAC), tools such as Kerberos, LDAP and Active Directory are used for establishing a single point of truth.

Regarding data protection at rest, different encryption schemes are used to protect against privileged users or applications with direct access to files with a central key management server. For data protection in transit, along with SSL/TLS protocol, native communication also requires encryption schemes such as remote procedure calls and socket communications [10]. All unencrypted data using different protocols such as DTP, HTTP, RPC, JDBC/ODBC need to be kept safe with privacy measures.

In order to achieve governance and auditing, different tools should produce uniform log information which could be analysed and could form business intelligence on top of the audit and governance data. The Risk and Governance (GRC) policies groups the sensitive data types in alignment with regulations by defining the rules to control the data flow (PCI,PII etc) for organization compliance[2][14].

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

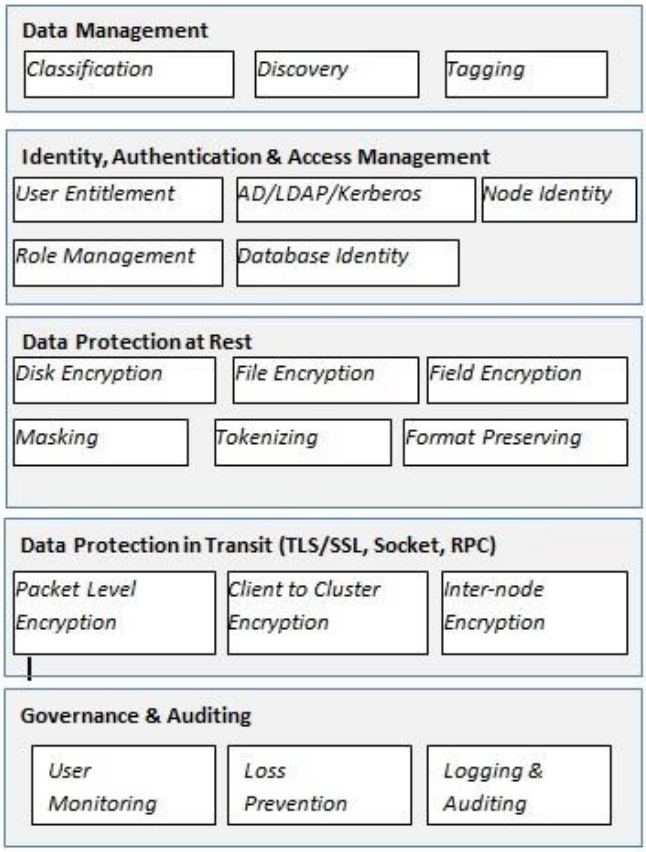


Figure 1: Proposed architecture for general security of data for big data.

G. *Existing Solutions for Securing Data in Transit*

AES (Advanced Encryption Standard) is the most widely used encyption scheme for data in motion.This scheme is used in most of the Big Data methodologies varying from authenticaiton, authorizaiton, SSL,TLS, socket data encryption to remote procedure calls. For example Kerberos strong authentication relies on the Kerberos tickets. By default, Kerberos will attempt to use 256-bit AES encryption with the Kerberos Ticket Granting Ticket [5]. Other encryption schemes are also used in Big Data, such as HMAC-SHA1, a symmetric key cryptographic algorithm distributing the symmetric key used in the HMAC-SHA1 to the Name Node and every Data Node in the cluster.

## III. Efficient Encryption Scheme For Big DATA

H. *Suitable Algorithm for Data in Motion*

Based on statistics and performance benchmarks [20][21][22][23][24][25], AES is found as the best in performance as well as strength in the family of symmetric cipher. Conventional AES has time complexity of $2^{48}$ and a memory complexity of $2^{32}$ [43]. Most of the latest Big Data implementation now supports standard AES algorithms with its key variants, modes and other parameters; besides the alternative and less secure standards such as 3DES and RC4. *Figure 2* shows the encryption performance of a conventional symmetric cryptosystems.

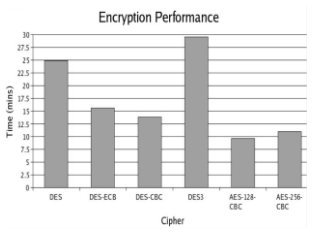


Figure 2: Performance of symmetric algorithms using OpenSSL with 8 gigabytes of data on a 1.0GHz Intel Server [23].

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

## B. AES Encryption Scheme and Computational Overhead

AES is based on Rijndael algorithm and has a fixed block size of 128 bits and a key length of 128, 192 or 256. It calculates a temporary round key from original symmetric key and it takes a 4x4 array (state) of data at a time and transforms the data using Round Keys. The process is repeated 10 to 14 times based on the block size. The transformation has four steps and the Galois Field (GF) calculation is used in steps. The first step in each cycle is called SubByte, which is substitution of values from an S-Box table calculated using special Galois Field mathematics. Secondly ShiftRow step re-orders shifting the data in a specific order. Third step is called MixColumn which will diffuse the data evenly to all the sections of the selected byte array using GF($2^8$) multiplication. Fourth step is AddRoundKey transformation where the round key, which is calculated from original symmetric key, is used for the key expansion and then resulting value is used for transforming state. *Figure 3* shows the common AES encryption/decryption process.
The traditional AES implementation using Galois Fields (GF) computes the GF($2^8$) multiplications. The storage requirement is from the 256-byte S-box and the main processing requirement comes from the GF($2^8$) multiplications of the one-time RoundKey and multi-time MixColumn operations[28].

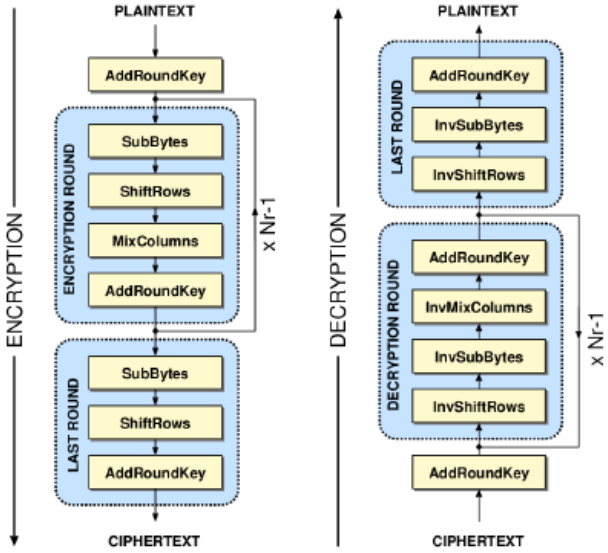


Figure 3: AES encryption & decryption Proc**ess**

## C. *AES Performance*

Network infrastructure, implementation algorithms, programming language used for implementation, key size, platform of choice, chipset for execution, processor and encryption hardware are the factors that affects the performance of the encryption and decryption of Data in Motion.

Figure 4 chart shows a benchmarking of different implementers on AES on the same environment and all other same parameters as an instance [24].

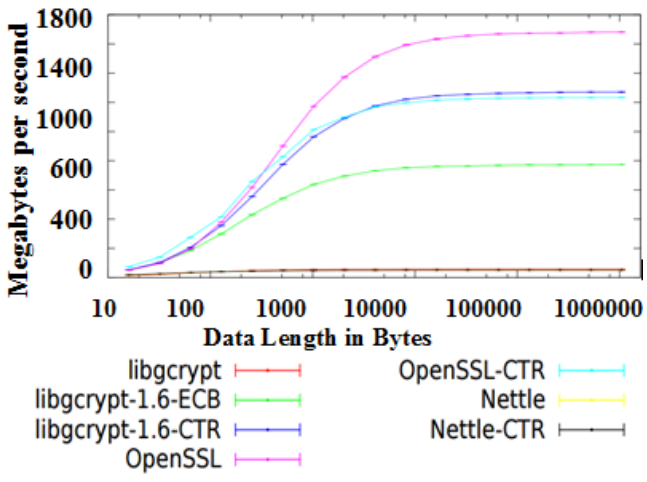


Figure 4: Performance of AES algorithm from different vendors using Ubuntu Intel Pentium 4 Systems [24].

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

D. AES Improved Performance and Optimization

From Big Data perspective, as data in motion is distributed in heterogeneous systems and complex network traffic with different network tools and solutions, it is quite challenging to formulate a method for having a high performing secure environment. A formula is proposed in this paper that can be adopted to provide a secure data in motion.

## IV. PROPOSED SYSTEM

Based on the literature survey and our experiments a simplified *Five Steps structure* has been proposed to achieve high performance in moving data in Big Data systems as illustrated in Figure 5. As we focus on the Data in Motion, majority of data in motion will be transferred using symmetric encryptions such as AES [29-35].

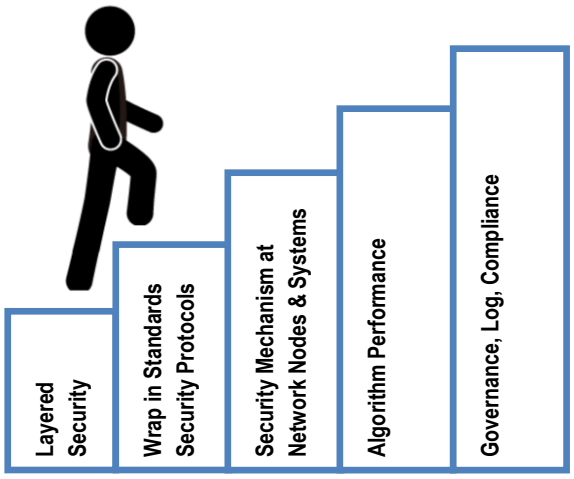


Figure 5: Proposed simplified Five Steps structure to achieve high performance in moving data in Big Data Systems

A. Layered Security

Apart from the network security layers explained in [32] and [33], Big Data implementation such as Hadoop provides security and privacy mechanism at different layers. These layers can be further tuned to make sure the confidential data is transferred after encryption. The layered structure will make sure which data need to be encrypted and which is not. Services like Key Management Server (KMS) store the keys including the temporal symmetric AES keys.
Integrity of network, servers and clients, security enforcement at various points in the network and implementation of security policies are also very important for a Big Data framework. Security effective processes, such as security policies, security awareness training and policy enforcement also need to be carried out for a successful layered security architecture [32][33][34][49].

B. Wrap Moving Data in Standard Security Protocols

Different layers of Hadoop facilitates secure file transfer (for instance FTP), secure query processing, secure message passing, secure control flow and secure data flow [49]. Wrapping these data using the well proven security protocol is very important in securing big data communications. For example Apache Knox for REST APIs for Hadoop will enable encrypted data moving over web. SSL and HTTPS provide AES key exchange securely so that the data transferred using AES algorithms will use temporary session key which will be destroyed after the communication. Available standards such as Java's Simple Authentication & Security Layer (SASL), Kerberos will help enforcing perimeter security with will provide authentication and strengthening authorization mechanisms. Current industry solutions are still using RC4 and 3DES[34] encryption schemes, but for secure communication it is always important to use unbreakable security using AES.

C. Security Mechanism at Network Nodes & Systems

Among many hardware solutions and accelerator [29][30] to support Big Data Security, Intel Advanced Encryption Standard New Instructions (AES-NI) and associated hardware framework provide support for Big Data Hadoop File System(HDFS). Data in transit performance could be achieved while encryption process happens between memory and HDFS file system. Intel AES-NI provides seven instructions that help to accelerate the most complex and compute-intensive steps of the AES algorithms [44][45]. Such solutions can be used at routers, nodes, access points where the machine crunching encryption and decryption happens with supporting protocols such as Network Security Services (NSS)[46][47][48] with support for SSL/TLS or similar standard protocols.

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

Alternatively, solutions such as using graphics card resources with a gKrypt Engine [26] will improve the speed of processing many times than executing the AES in normal processor.

D. Algorithm Performance

There are many improvements and variations to AES algorithm suggested such as Dual Key[42], Single Lookup Table (LUT) [28], AES Hybrid Approach[51], AES Lightweight models, optimized software solutions for multi-core platforms [38-41].
The Single lookup AES reduce the processing steps on the GF lookup table. This method needs only 16 Load operations and 16 XOR operations to compute the new state, and consumes just about 1/100 of cycles consumed by GF($2^8$).
As explained in the section "AES performance", selecting the right implementation and vendor suitable for the platform of choice is very important.

E. Governance, Log, Compliance

Monitoring the network traffic for possible intrusion and flows, keeping an eye on new possible threats, enable regular security updates on systems, installing a data protection solution are all equally important. A new style of intrusion prevention system (IPS) similar to that of normal data flow still needs to be evolved for systems like Hadoop [32-33].

## V .Conclusion And Future Work

Securing data in motion is very important in Big Data implementations. After looking at the available literature, a global standard and formula to make the moving data secure is found to be not available. Here we attempted to propose a simplified framework and formula to make the data in motion secure in Big Data scenario with a focus on AES structure.
As authors are participants of National Institute of Standards and Technology (NIST) Big Data Working Group (NBD-WG), further study and framework components will be added in the global standard specific to the subject. The version 2 of the NIST Big Data interoperability Framework (NBDIF) might include such components, which is planning to be started by middle of 2015.

## VI . References


[1] Vijaykumar Patil1, Prof. Venkateshan, *"Review on Big Data Security in Hadoop",* Department of Computer Engineering, University of Pune SKN'Sinhgad Institute of Technology and Science, Lonavala, Pune, Maharashtra, India.
[2] Owen O'Malley, "Integrating Kerberos into Apache Hadoop", Yahoo's Hadoop Team, Kerberos Conference 2010
[3] Xuefu Zhang |Software Engineer, Cloudera, "Secure Your Hadoop Cluster With Apache Sentry",Cloudera, April 07, 2014
[4] Hortonworks, "Hortonworks Data Platform : Hadoop Security Guide", Copyright © 2012-2014 Hortonworks, Inc. Some rights reserved.
[5] Andrew Becherer, "Hadoop Security Design Just Add Kerberos? Really?", iSEC Partners, Inc., Black Hat USA 2010.
[6] Owen O'Malley, Kan Zhang, Sanjay Radia, Ram Marti, and Christopher Harrell "Hadoop Security Design", https://issues.apache.org/jira/secure/attachment/12428537/security-design.pdf
[7] Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters", http://labs.google.com/papers/mapreduce.html
[8] Aaron Cordova "MapReduce Over Tahoe", http://code.google.com/p/hadoop-lafs/wiki/HadoopTahoeSecureConfig
[9] Cloudera , "CDH 5 Security Guide", Version: 5.1.x, (c) 2010-2014 Cloudera, Inc. All rights reserved, September 23, 2014
[10] Ajit Gaddam, "Data Security in Hadoop", Strata Conference, Strata Hadoop.
[11] EMC Corporation, Whitepaper: "Security and Compliance for Scale-out Hadoop data lakes", August 2014
[12] Stuart Rogers & Tom Keefer, Best Practices, "Hadoop with Kerberos – Deployment Considerations", SAS Institute Inc, USA, 2014.
[13] Zettaset Whitepaper, "The Big Data Security Gap: Protecting the Hadoop Cluster", Zettaset USA, 2013.
[14] DATAGUISE, Whitepaper, "SECURING HADOOP: DISCOVERING AND SECURING SENSITIVE DATA IN HADOOP DATA STORES", www.dataguise.com, 2012.
[15] Cloudera Whitepaper, "SECURING YOUR ENTERPRISE HADOOP ECOSYSTEM : Realizing Data Security for the Enterprise", Cloudera, 2012.
[16] "How-to: Set Up a Hadoop Cluster with Network Encryption" http://blog.cloudera.com/blog/2013/03/how-to-set-up-a-hadoop-cluster-with-network-encryption/
[17] White Paper: "Increase the Value and Relevance of Data in Motion", Cisco, 2013. http://unleashingit.com/docs/B13/IoE%20Data%20Motion/increase_the_value_relevance_of_data_in_motion.pdf
[18] Tom Bowers, "How to Lock Down Data in Motion", Information Security Magazine, SearchSecurity.com.
[19] Sowmya Nag, H.B.Bhuvaneswari, Nuthan A.C, "IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD-192 BIT USING MULTIPLE KEYS", AMC Engineering College.
[20] "Using Engine_cudamrg with the OpenSSL", https://code.google.com/p/engine-cuda/wiki/benchmarkVersion011, Jan 13, 2011.


**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

[21] Article by Bingmann, "Speedtest and Comparsion of Open-Source Cryptography Libraries and Compiler Flags", https://panthema.net/2008/0714-cryptography-speedtest-comparison/, 2008.
[22] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/
[23] Kerry Thompson, "Backup Encryption", SysAdmin Magazine, http://www.crypt.gen.nz/papers/backup_encryption.html March 2007.
[24] Werner Koch, "Speedups in Libgcrypt", https://www.gnupg.org/blog/20131215-gcrypt-bench.html , 15th December 2013. Statistisc: http://koti.kapsi.fi/~jukivili/gcrypt/haswell-3200-ubuntu-saucy-gcrypt.pdf
[25] Nikos Mavrogiannopoulos, "TLS in embedded systems", http://nmav.gnutls.org/2012/04/in-some-embedded-systems-space-may.html, April, 2012.

[26] gKryptEngine, "Lightening fast, military grade crypto module" , http://www.gkrypt.com/engine/
[27] Implementation of AES in Java :
http://cryptm.org/~josh/src/AES.java , https://dl.dropboxusercontent.com/u/31222469/blog/crypto/AES.java
https://en.wikipedia.org/wiki/AES_implementations
http://wiki.secondlife.com/wiki/AES_Java_Implementation
[28] Xinqiang Luo, Yue Qi, Yadong Wan, Qin Wang: "A Fast AES Encryption Method Based on Single LUT for Industrial Wireless Network", University of Science and Technology Beijing, China, 2014.
[29] Rahimunnisa K, Karthigaikumar P, Kirubavathy J, et al. A 0.13-
μm implementation of 5 Gb/s and 3-mW folded parallel architecture for AES algorithm[J]. International Journal of Electronics, 2013
[30] Morioka S, Satoh A. A 10-Gbps full-AES crypto design with a twisted BDD S-Box architecture[J]. IEEE Transactions on VLSI Systems, 2004.
[31] Leslie Xu. Secure the Enterprise with Intel® AES-NI: WhitePaper. http://www.intel.cn/content/www/cn/zh/enterprisesecurity/enterprise-security-aes-ni-white-paper.html
[32] Pamela Warren, Nortel Corp, "Ten steps to secure networking" http://www.computerworld.com/article/2559866/security0/ten-steps-to-secure-networking.html
[33] Michael Sanchez, "6 Steps for Ensuring Small Business Network Security" http://blogs.cisco.com/smallbusiness/6-steps-for-ensuring-small-business-network-security
[34] Vinay Shukla, "Wire Encryption in Hadoop", http://hortonworks.com/blog/wire-encryption-hadoop/, December, Hortonworks, 2013.
[35] "Transparent Encryption in HDFS", http://hadoop.apache.org/docs/r2.7.0/hadoop-project-dist/hadoop-hdfs/TransparentEncryption.html, Apache.org, April 2015.
[36] Coudera ,"Configuring Hadoop Security in CDH4", AES Installation Guide, http://www.cloudera.com/content/cloudera/en/documentation/cdh4/v4-3-1/CDH4-Security-Guide/cdh4sg_topic_3_3.html
[37] https://www.ietf.org/rfc/rfc3394.txt https://en.wikipedia.org/wiki/Key_Wrap
[38] HortonWorks, "Comprehensive and Coordinated Security for Enterprise Hadoop", http://hortonworks.com/innovation/security/
[39] Bertoni G, Breveglieri L, Fragneto P, et al. Efficient software implementation of AES on 32-bit platforms[M]//Cryptographic Hardware and Embedded Systems-CHES 2002. Springer Berlin Heidelberg, 2003.
[40] B. Gladman. A Specification for Rijndael, the AES Algorithm. Available at http://fp.gladman.plus.com, May 2002.
[41] Atasu K, Breveglieri L, Macchetti M. Efficient AES implementations for ARM based platforms[C] //Proceedings of the 2004 ACM symposium on Applied computing. ACM, 2004.
[42] Abhiram.L.S, Gowrav.L, Punith Kumar.H.L ,"Design and synthesis of Dual Key based AES Encryption", M.S.Ramaiah Institute of Technology, Bangalore, India, 2014.
[43] Vincent Rijmen. "Practical-Titled Attack on AES-128 Using Chosen-Text Relations", 2010. http://eprint.iacr.org/2010/337.pdf
[44] Whitepaper from Iddo Kadim, Director of Datacenter Technologies, Intel Corporation "Fast, Low-Overhead Encryption for Apache Hadoop" , 2013.
[45] Whitepaper from Intel and Coudera, "Intel® Xeon® Processor E5-2600 v3 Accelerates Hadoop HDFS Encryption", http://www.intel.com/newsroom/kits/xeon/e7v3/pdfs/Xeon_E7v3_Cloudera-aes-ni.pdf, 2015.
[46] "Network Security Services" - Developers Web Page, https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS, mozilla.org Projects.
[47] Article: "AES-NI SSL Performance a study of AES-NI acceleration using LibreSSL, OpenSSL", https://calomel.org/aesni_ssl_performance.html, April 24, 2015.
[48] Design Doc DRAFT, "Chrome: From NSS to OpenSSL", Last edited on: 2014-01-26. https://docs.google.com/document/d/1ML11ZyyMpnAr6clIAwWrXD53pQgNR-DppMYwt9XvE6s
[49] Whitepaper from IGATE, "A Quick Look at Hadoop Security" http://www.igate.com/documents/11041/0/Big_Data_Security_A_Quick_Look_At_Hadoop_Security.pdf

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.

[50] Grant, "Hardware AES Showdown - VIA Padlock vs Intel AES-NI vs AMD Hexacore", http://grantmcwilliams.com/tech/technology/387-hardware-aes-showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore, July 6, 2011.

[51] Ooi Bee Sien, Azman Samsudin, and Rahmat Budiarto, "A New Image-Database Encryption Based On A Hybrid Approach of Data-at-Rest and Data-in-Motion Encryption Protocol" , Universiti Suins Malaysia

**Cite this article as:** Sarafudheen M Tharayil, K.Kalaiselvi, Dr. Paul Rodrigues, Dr. Anand Kumar. "Enhancing Performance and security for 'Data in Motion ' in BIG DATA." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 32-39. Print.