Implementation And Performance Analysis of Proposed Security Framework For Uidai

Dr. Arpana Chaturvedi

Asst. Prof. & Department of Information Technology & Jagannath International Management School, Vasant Kunj, New Delhi, India

Abstract* — *The development of new technologies like Hadoop, Map Reduce, used to store, manage, analyze vast amount of data, when associated with WSN (Wireless Sensor Network), the risk factor for information security increases. When it is applied in various applications of government like Aadhaar, DigiLocker etc., chances of hidden security issues increased. In this paper AES-XTS encryption mechanism and digital signature technology is used with AODV (Ad hoc On-Demand Distance Vector) routing protocol to get rid of various issues like DoS (Denial of Service), eavesdropping, imitation, coaxing etc. The theoretical analysis is shown using NS2 simulator and implementation assures to provide better data security, reliability, transmission and energy efficiency. This implementation shows that SAODV(Secure-AODV) routing protocol when used in routing layer in these applications and system, it increases its own self defensive ability to fight against various challenging hidden security issues.

Keywords - *AODV, SAODV, WSN, AES-XTS, UIDAI, DoS.*

I. INTRODUCTION

The UIDAI (Unique Identification Authority of India) data, both at rest or on move, stored at CIDR (Central Identities Data Repository) is at high risk. Due to the advent of new Hacking technologies and advanced tools, the risk factor has increased. The government is enforcing citizen of India to link Aadhaar number with different citizen centric services so that right citizen can avail the benefits. There is need to safeguard the data stored in different data centres which might be secured through a strict encryption technique applied on application process in parallel mode. In this chapter, an encryption process to be performed in parallel mode is discussed. The proposed approach is AES in XTS Mode in Map Reduce paradigm which supports parallel programming in the distributed environment. The findings after reviews of results show that it provides better security against external attacks and overcomes the shortcomings of Kerberos. Encryption followed by compression on various datasets provides better result and protection from vulnerabilities and threats.

With the development of wide application of WSN (Wireless Sensor Network) and advanced technologies, the risk to the information security in various government and private sector has increased. Here we integrate the AES encryption standard in XTS mode and digital signature technology to improve classic AODV (Ad hoc On-Demand Distance Vector) routing protocol. The resultant SAODV (Secure Ad hoc On-Demand Distance Vector) routing protocol provides better information security and achieves energy efficiency as well. In this chapter, we reviewed different observations and it is concluded that the algorithm is an appropriate choice.

The chapter is divided into further four sections. Section II explains the requirement of strict encryption algorithm in current scenario. The concept is suggested with respect to the requirement of security approaches for the UIDAI System. Section III describes the importance and benefits of AES-MR technique highlighting the XTS encryption Mode. Section IV shows the experimental results are explained using implemented simulation environments. It highlights the benefits of using this approach to secure sensitive information. The chapter is finally concluded in Section V.

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. REQUIREMENT OF STRICT ENCRYPTION OF DATA

Since ages data collection has increased enormously with high velocity. 80% of the total data is collected just during the last two years. This extraordinary growth in data generated is due to miscellaneous activities performed by common man. The advent of technologies like cloud computing, active use of social media, mobile computing, internet of things, sensor-based network etc. requires large and efficient storage with security. This advancement in technology increases the generation of data exponentially and need strict security strategies to be implemented in the system. The sensitive data are stored in various datacenters. The government initiated the concept of Digital India and enforces end users to link their Aadhaar number with various services. UIDAI system and related infrastructure have already implemented strong security authentication and compliances. With the pace, speed, and momentum the citizens are enforced to link their Aadhaar number with various services to avail benefits, their concern about the breach of privacy of their data has increased. Citizens of India have submitted their demographic and biometric details to the UIDAI system. To avail benefits, their personal data need to be shared among different agencies. They need assurance that the data will not be misused. Many issues in past were raised regarding misuse of private information, leakage of private information and theft of data. IBM estimates that 90% of the world's data was generated in the last few years alone which has increased the reliability and security challenges to keep safe and secure the enormous data. Major challenges are related to reliable storage, efficient processing, data integrity, and recovery. It is necessary to modify the existing security compliances, legal provisions, and auditing policies.

There are so many technologies and algorithms available which might be appropriate to handle security issues. The study concludes that the implementation of AES-XTX with map reduce parallel programming will be a cost-effective solution to process such a large user-generated vital and sensitive data.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

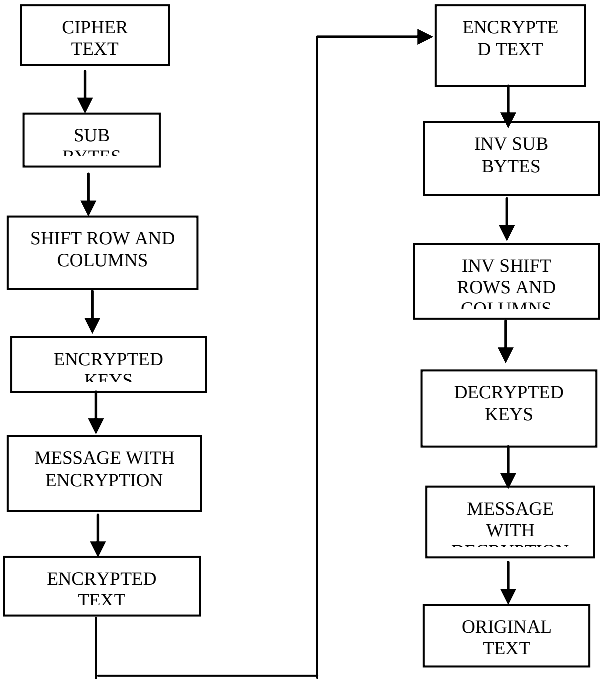


Fig 1 Encryption and Decryption Process

III. AES-MR

The combination of Advanced Encryption Standards (AES) and Map Reduce (MR) is termed as AES-MR. It is the proposed algorithm for this research work which is related to the case study done for UIDAI to provide better data security. This encryption algorithm is proposed to provide Data level security. Map Reduce is a parallel programming language and AES is the encryption algorithm suitable for longer messages. It is suggested that the best features of both techniques should be used together to provide much stricter security features in the introduced security layer.

Map Reduce with AES-XTS has the capability to compose applications that generates endless data during runtime. It has the ability to adapt non-critical failures and can perform better planning, testing of information. The failed jobs if encountered in the clusters of machines, it re-executes them.

PROPOSED ENCRYPTION ALGORITHM-AES (XTS)-MR

In this proposed technique AES is used with XTS mode which is supported by IEEE 1619-2007 standards [5]. The XTS modes contain XEX-TCB-CTS (XTS) mode where XTS stands the XEX Tweakable Block Cipher with Cipher Text Stealing. The XTS mode performs parallel executions and allows pipelining in respective executions. Data Encryption Standards which were used earlier is vulnerable to Brute Force attacks. It was due to the small size of the key (53 to 2054 bits) DES uses for encryption. US Government Agency NIST (National Institute of Standards and Technology) selected Rijndael's Algorithm as Advanced Encryption Standard. It is being a better security standard now becoming an Industry Standard.

AES is designed to accept 128, 192, 256 bits' size of keys. These various sizes of keys are capable of encrypting different types and variety of information in bulk. The performance of AES algorithms varies on different 32 bit and 64-bit CPU's based on key sizes. This technique will provide better security (Fig.2) in case of the UIDAI system where the large data sets are generated for storing sensitive information of residents and generating UID numbers of a citizen of India.

The block contents can perform parallel processing in various modes of operations. These operations can handle fixed block as well as variable block encryption with the help of single key or different keys.

XTS ENCRYPTION MODE

The Electronic Cook Book (ECB) and XTX are used with AES to increases the effectiveness of an algorithm and can be improved by the use of it. [5] The XTX supports parallel encryption mode with Symmetric Block Cipher encryption mode. It was designed to protect data lying at rest on storage devices.

It uses a fixed size of data units to perform cryptographic protection of data at rest. The operation of AES-XTX Mode with two different keys is shown in Fig. 3 [12] [5]. The XTS-AES mode is an enhanced concept of Rogaway's XEX (XOR Encrypt XOR) Tweakable Block Cipher, improved with a method called "Cipher Text Stealing". It expands the range of possible different types of data inputs. XEX can only encrypt sequences of complete blocks of any data type. This input data should be an integer and necessarily be a multiple of 128 bits. In XTS-AES, the data string consists of one or more complete blocks which are followed by a single, non-empty partial block ().

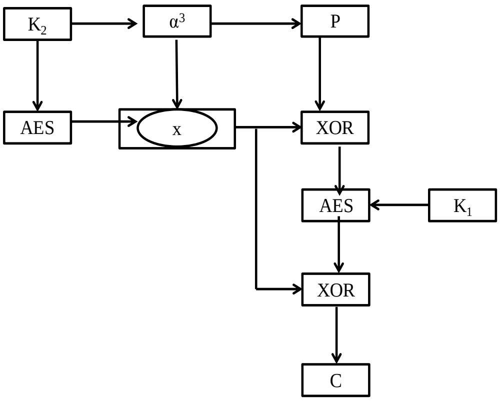


Fig.2 Operation of AES-XTX Mode with two different keys

The working of AES-XTS is shown in Fig. 3. The XTS-AES is composed of two keys, first one is an encryption key and second one is tweak key. It incorporates the logical position of the data block into the encryption [11]. The output produced by XTS is independent which leads to parallelization. XTS, an instantiation of the tweakable Block Cipher class. It is capable to implement ciphers in parallel and pipeline modes. It enables the encryption of the last incomplete block also.

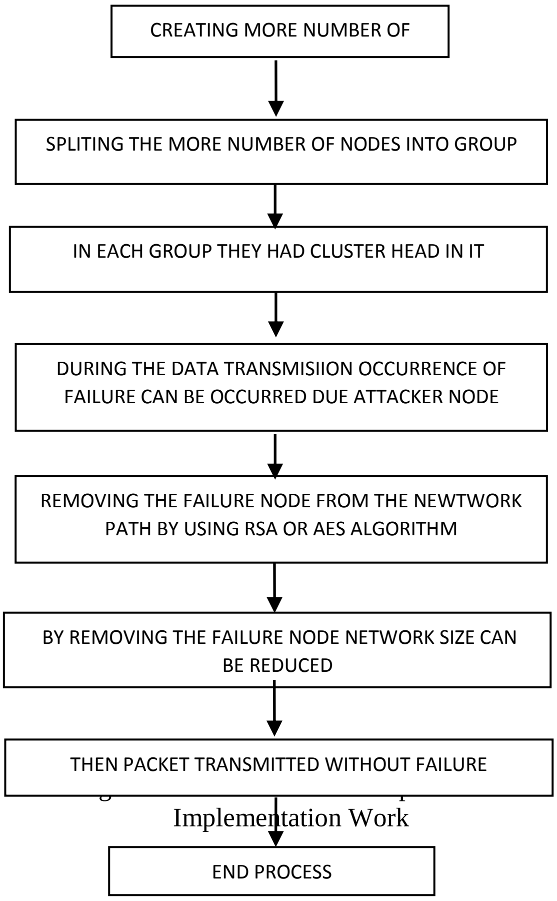
IV. EXPERIMENTAL RESULT AND ANALYSIS

The experimented results are drawn are done using various randomly created sizes of datasets. This work integrates the international popular AES-XTS encryption standard to improve existing AODV routing protocol, and uses improved, energy efficient SAODV routing protocol to provide better information security. The details of the simulation environment used to show the proposed implementation work is shown in Table 1.

CPU type	Intel® Core™ i5 4210U
Clock speed	CPU ®@2.40 GHz
Ram size	16 GB RAM x-64- based processor
Operating System	Ubuntu Server Basic, 64 Bit Windows 7 Home.
Framework	Hadoop Framework
Simulation Tool	NS2
Tools	Ms. Office, MS Excel
Language	Java, , JDK1.8,

Table 1 Details of Simulation Environment

The theoretical analysis and simulation shows the better performance of SAODV by adding proposed security mechanism to AODV in the routing layer. The steps of implementation work are shown in Fig. 3.


CREATING MORE NUMBER OF
SPLITING THE MORE NUMBER OF NODES INTO GROUP
IN EACH GROUP THEY HAD CLUSTER HEAD IN IT
DURING THE DATA TRANSMISIION OCCURRENCE OF FAILURE CAN BE OCCURRED DUE ATTACKER NODE
REMOVING THE FAILURE NODE FROM THE NEWTWORK PATH BY USING RSA OR AES ALGORITHM
BY REMOVING THE FAILURE NODE NETWORK SIZE CAN BE REDUCED
THEN PACKET TRANSMITTED WITHOUT FAILURE
END PROCESS

Implementation Work

DESCRIPTION OF ROUTING PROTOCOL AND ITS ASSIGNED PROTOCOL

The routing protocol used in this simulation environment to show implementation and other details are shown below in the Table 2 as:

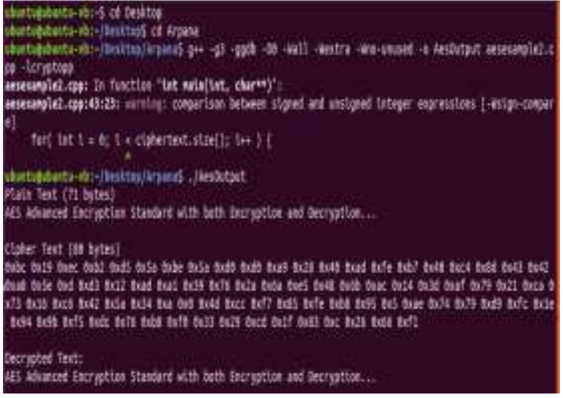
Routing Protocols	Remarks
Number of nodes used	31
Node act as source node	Node 2
Node act as destination node	Node 21, 15, 19
Node act as cluster head	Node 4, 9, 16, 26
Mobility speed	10mps
Simulation time	25ms
Transmission range	300m
Mobility movement	Random path
Transmission range	2packets/sec
Number of connection	5 connections
Buffer size	128 packets
Number of graphs	6

Table 2: Description of Routing Protocol and assigned protocol

USING AES ALGORITHM

In the below shown screenshot (Fig. 5), it clearly gives the explanation of the process of encryption and decryption by using AES method has been explained. Thus in this first we used plain text after encryption process can be occurred and convert the message into cipher text.

At final receiver want to receive the original message thus the decryption had been occurred and convert cipher text message to original message.



```
ubuntu@ubuntu-vb:~$ cd Desktop
ubuntu@ubuntu-vb:~/Desktop$ cd Arpana
ubuntu@ubuntu-vb:~/Desktop/Arpana$ g++ -g3 -ggdb -O0 -Wall -Wextra -Wno-unused -o AesOutput aesesample2.c
pp -lcryptopp
aesesample2.cpp: In function 'int main(int, char**)':
aesesample2.cpp:43:23: warning: comparison between signed and unsigned integer expressions [-Wsign-compar
e]
    for( int i = 0; i < ciphertext.size(); i++ ) {
                      ^
ubuntu@ubuntu-vb:~/Desktop/Arpana$ ./AesOutput
Plain Text (71 bytes)
AES Advanced Encryption Standard with both Encryption and Decryption...

Cipher Text (88 bytes)
0xbc 0x19 0xec 0xb1 0xd5 0x5a 0xbe 0x5a 0xd0 0xd0 0xa9 0x28 0x40 0xad 0xfe 0xb7 0x48 0xc4 0xd8 0x43 0x42
0xa8 0x5e 0xd 0xd3 0x12 0xad 0xa1 0x19 0x76 0x2a 0xba 0xe5 0x48 0xbb 0xac 0x14 0x3d 0xaf 0x79 0x21 0xca 0
x73 0x30 0xc0 0x42 0x1a 0x14 0xa 0x0 0x4d 0xcc 0xf7 0x85 0xfe 0xb8 0x95 0x5 0xae 0x74 0x79 0xd9 0xfc 0x1e
 0x94 0x6b 0xf5 0xdc 0x76 0xb8 0xf0 0x33 0x29 0xcd 0x1f 0x81 0xc 0x26 0xb8 0xf1

Decrypted Text:
AES Advanced Encryption Standard with both Encryption and Decryption...
```

Fig. 5. Screenshot of command used to execute the implementation work

OUTPUT OF IMPLEMENTATION WORK

The various output of the implementation work is shown below in the sequence of implementation of work performed.

A. NODE FORMATION

The formation of nodes is shown here. In this the total number of nodes used are 31. Among these 31 nodes, four nodes are used as a cluster node. These are node 4,9,16 and 26. The node which acts as a source node is 2. The nodes which acts as a destination nodes are 21,15 and 19. The mobility speed 10 mpbs. The simulation time is 25ms and the transmission range is 300m. The total number of connections used in the implementation are 5 with random mobility movement. The transmission range is 2 packets per second with buffer size of 128 packets. The four channels ch1 as node 4, ch2 as node 9, ch3 as node 16 and ch4 as node 26 are used with Key exchange node as node 7. The total number of graphs shown here are 6.

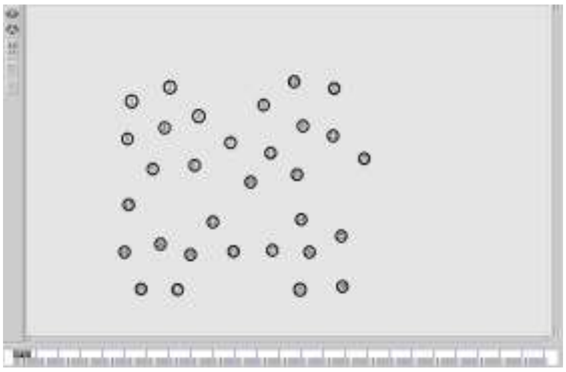


Fig. 7. Screenshot which show Node creation

In the above screenshot (Fig. 7) node creation has been occurred. In this network number of node created is 30.

B. ALLOCATION OF SENDER AND RECEIVER FOR VARIOUS NODES

In the below (Fig. 8) screenshot for the formation of group of nodes it had been assign the cluster head with source and destination.

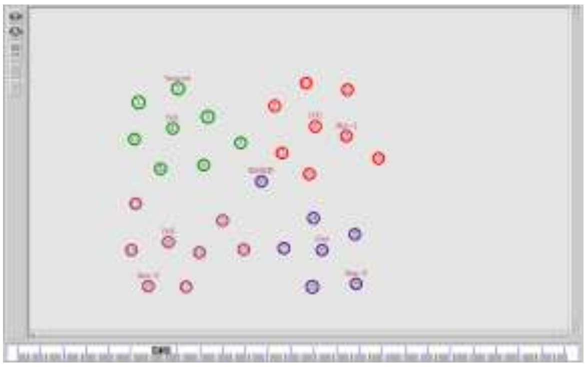


Fig. 8. Assign the cluster head with source and destination

C. DATA TRANSMISSION

In this graph (Fig. 9) it has shown that how TCP/IP protocol is selected among various channels. The total channels used here are 4. These are as Ch1, Ch2, Ch3 and Ch4 as node 4, node 9, node 16 and node 26 respectively.

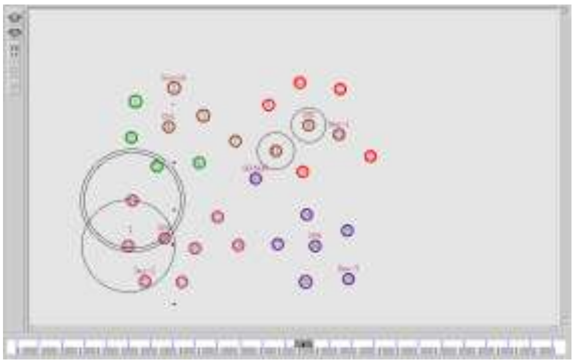


Fig. 9. Selection of Channel by TCP/IP Protocol

In the above after the assigning of cluster head, source and destination the process of transmission had been occurred. While transmitting the data loss may be occurred due to this security of the network had been occurred problem.

D. TRANSMISSION WITH KEY EXCHANGE

In this graph (Fig. 10) the key exchange node is identified as node 7. It is responsible for exchange of keys while transmission of packets from single source to multiple destinations. It performs encryption and is known to sender and receivers only. As during transmission only, the key exchange node is identified, it is very difficult for hackers to identify it. In this way it provides better security implementation.

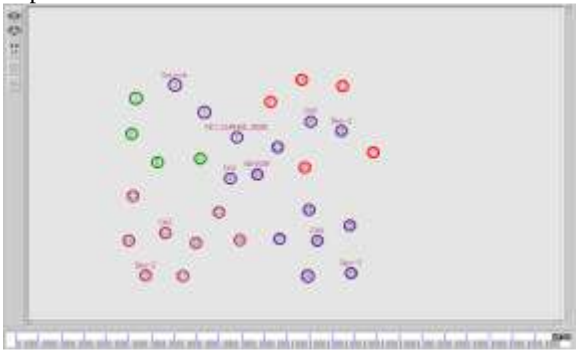


Fig. 10. Transmission of Information with Key Exchange

In the above screenshot due to the occurrence of loss we want to reduce that loss and improve the security of network. We can use the AES algorithm in which while transmitting the data, key had been used to improve the security without any loss in the network.

GRAPH REPRESENTATION

The various output obtained after implementation of proposed technique is shown below in the form of graph as:

A. DROP IN DATA

In this graph (Fig. 11) the packet drop has been showed between both existing and proposed method. Packet drop has been calculated by number packets drop in network while transmitting the data between the different nodes.

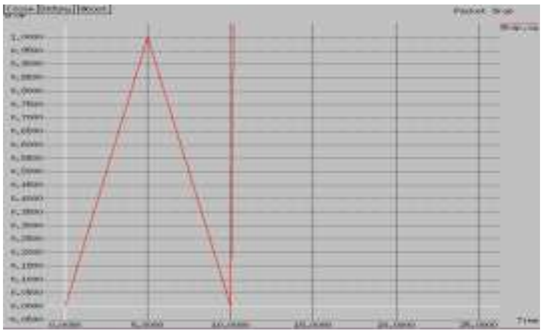


Fig. 11. Packet drop between the Existing and Proposed Method

B. DATA TRANSMISSION IN ENCRYPTION

In this graph (Fig. 12) the filtering of nodes and packets are shown. It checks the packets which are manipulated while transmission by some intruders, hacker’s r or by eavesdropping. It does not allow the corrupted packets as removes them and passes rest of the filtered packets. It also checks the nodes. If some nodes through which packets are transmitted are not authorized and registered, it removes it from the channel.

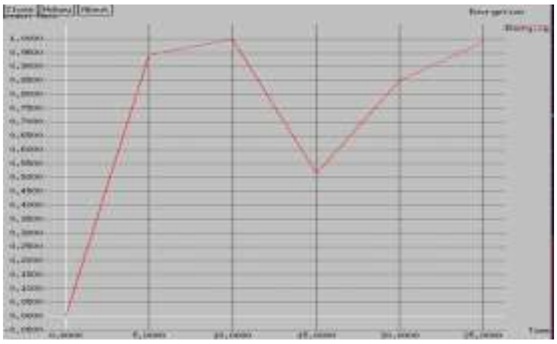


Fig. 12. Filtering of Nodes and Packets

In this graph the data encryption has been showed while transmitting the data. When the sender sends the original data by using encryption process data can be converted to cipher text. During the process encryption of the data in network has been calculated.

C. DATA DECRYPTION WHILE DATA TRANSMISSION

In this method data is decrypted while transmission of data to provide better security using AES technique.

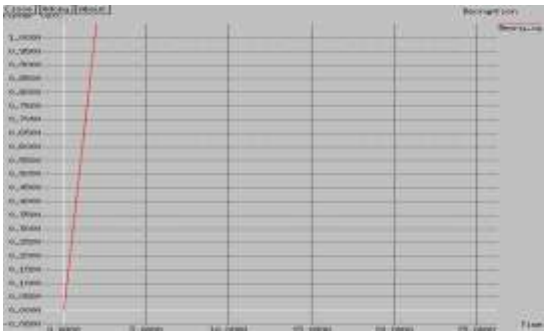


Fig. 13. Data Decryption while Transmission of Information

In this graph (Fig. 13.) the data decryption has been showed while transmitting the data. Thus after the process, of encryption data want to decrypt to plain text for the receiver view. Thus data transmission has been calculated in decryption.

D. COMPARISON FOR LOSSES IN PACKETS IN EXISTING VS PROPOSED

The loss of data has been showed while transmitting the data. It is identified by particular amount of data loss and filtering of nodes.

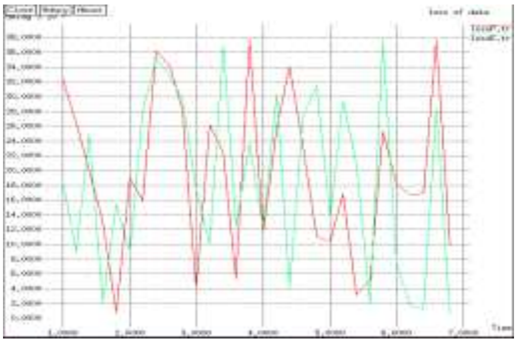


Fig. 14. Loss of Data while Transmission of Information

In this graph the loss of data has been showed while transmitting the data. When the data transmitted from sender to receiver, the particular amount loss in data has been occurred. Thus it has been calculated and shown in the graph in the relation of existing and proposed method

E. DATA PACKET TRANSMISSION IN VARIOUS NODES

The data transmission has been showed while transmitting the data in various nodes. Sender sends the data packets n various nodes and it is clear through graph (Fig. 15) that more packets are transmitted in case of proposed methodology in comparison to the existing one. It has shown a 95% of difference in number of data packets transmitted in various nodes and increases the speed of transmission also.

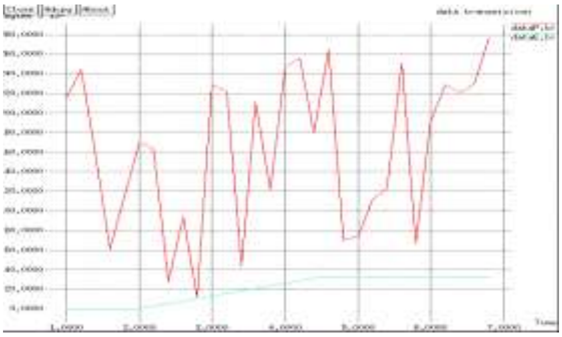


Fig. 15. Increased speed when Data Packets transmitted through Various Nodes

In this graph the data transmission has been showed while transmitting the data from sender to receiver.

F. Passing of Data with Individual Key Values

In this graph (Fig. 16) it's clearly shown that when data passed or transmitted through different channels in the form of packets, using AES-XTS encryption methodology and using key exchange according to this encryption technique, provides better transmission in comparison to existing encryption techniques. The comparison shows the 95% of betterment and difference in transmission with individual key values. This proposed encryption technique results in better security implementation in comparison to existing mechanisms

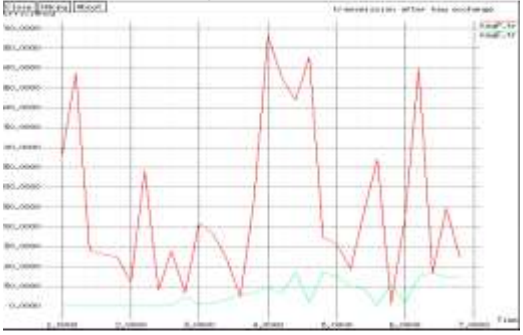


Fig.16. Comparison of Security implementation in Existing and Proposed Mechanism

In this graph the data transmission has been showed while transmitting the data from sender to receiver in the presence of key.

V. Conclusion

In this work we suggested AES-MR encryption technique to be implemented to solve the issue of data security at the storage level i.e. on HDFS (Hadoop Distributed File System). It is done by encrypting the data using AES-MR(XTX) along with compression at Mapper and Reducer phase. AES-MR(XTX) will not only enhanced the security of important data at HDFS level, but with the help of parallel processing we can do it with a faster manner as well.

With the help of simulation using NS2 simulator it is concluded that as the security is key anxiety of the wireless network which transfer data from nodes towards other. In the existing work, the performance of MANET is considered by using different parameters such as Network Overhead, Delay and Throughput. There are a few nodes which increase the system transparency, Delay and reduce Network throughput they are famous as malicious nodes. In proposed work, we used AES algorithm in WSN and then encryption to expand the demand or of network. In the future this approach can also be used to get better security in other networks like VANET, SPANs etc. it has been concluded that AES encryption standard when used in XTS mode will give better results in terms of security, Speed of transmission, better filtration of packets and Nodes. This technology can be used in various services provided by government now-a-days where it became mandatory to use Aadhaar card to link with the services to avail benefits. The block size used in AES is comparatively larger and varied, depending upon the requirement. The encryption process of XTS mode in AES is also complex that hackers cannot easily hack the transmitted crucial information. We can conclude that as AES-MR (XTS) helps to attain all the levels of security that too at a faster speed, it is a good approach.

ACKNOWLEDGMENT

This research was supported by various research work done by researchers and published papers. I thank all of them as their research work has provided the insight and expertise to me and their work has greatly assisted my research. I would like to thank and show my gratitude to Dr. Vinay Kumar and Dr Meenu Dave for sharing their pearls of wisdom with me during the course writing this research paper. I am immensely grateful to the reviewers for their comments on an earlier version of the manuscript, although any errors are my own and should not tarnish the reputations of these esteemed persons

REFERENCES

[1] Kadre V., Chaturvedi S., “AES – MR: A Novel Encryption Scheme for securing Data in HDFS Environment using Map Reduce”, www.ijcaonline.org/ research/ volume129/ number12/kadre-2015-ijca-906994.pdf

[2] Mehak, Gagan, “Improving Data Storage Security in Cloud using Hadoop “, ISSN: 2248-9622, Vol. 4 , Issue 9(Version 3), September 2014, pp.133-138,http://www.ijera.com/papers/Vol4_issue9/Version%20 3/U4903133138.pdf

[3] Weeks B., Bean M., Rozylowicz T., Ficke C.,” Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms, National Security”, https:// csrc.nist.gov/CSRC/ media/ Projects/ Cryptographic-Standards-and-Guidelines/documents/aes-development/NSA-AESfinalreport.pdf doi=10.1.1.35.6941

[4] Clunie D., Public Comments on the XTS-AES Mode,” https://csrc.nist.gov/csrc/media/projects/.../comments/xts/collected_xts_comments.pdf

[5] Public Comments-Modes Development - Block Cipher Techniques, "https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Public-Comments-Modes-Development“,Comments submitted to Encryption Modes @nist.gov.

[6] Dr. Hawthorne, NY, Computing Arbitrary Functions of Encrypted Data Craig Gentry IBM T.J. Watson Research Center 19 Skyline,cbgentry@us.ibm.com https://crypto.stanford.edu/craig/easy-fhe.pdf.

[7] Desai Spark Y., Gao J., Sang-Yoon Chang, Chungsik Song, “Improving Encryption Performance Using Map reduce”, Published in: High Performance Computing and Communications (HPCC), IEEE 17th International Conference, ISBN: 978-1-4799-8937-9, http:// ieeexplore. ieee.org / document/7336355/

[8] G. Sujitha, M. Varadharajan, B. Raj Kumar and S. Mercy Shalinie ,”Provisioning Mapreduce for Improving Security of Cloud Data “,http:// scialert.net/ qredirect.php? doi = jai.2013.220.228& linkid=pdf, International Journal of Computer Science and Applications, © Technomathematics Research Foundation Vol. 13, No. 2, pp. 89 – 105, 2016.

[9] Alexander Uskov, Adam Byerly, Colleen Heinemann,” Advanced Encryption Standard Analysis with Multimedia Data on Intel® AES-NI Architecture”, Research Institute Bradley University, 1501 West Bradley Avenue Peoria, Illinois 61625, U.S.A. auskov@bradley.edu http://www.tmrfindia.org/ijcsa/v13i26.pdf

[10] Demir L., Thiery M., Roca V., Jean-Louis Roch, Jean-Michel Tenkes, “Improving dm-crypt performance for XTS-AES mode through extended requests “, Nov 21, 2016 The 4th International Symposium on Research in Grey-Hat Hacking - aka GreHack, Nov 2016, Grenoble, France https://hal.inria.fr/hal-01399967

[11] Philip Derbeko, Shlomi Dolev, Ehud Gudes, Shantanu Sharma” Security and Privacy Aspects in map reduce on Clouds: A Survey”, www.https://arxiv.org/abs/1605.00677, www.iiste.org, ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012

[12] Liskov M., Mine Matsu K., “Comments on XTS-AES” September 2, 2008 This is a comment in response to the request for comment on XTS-AES, as specified in IEEE Std. 1619-2007 September 2, 2008, https://csrc.nist.gov/csrc/media/ projects /block-cipher-techniques/ documents/ bcm/ comm. ents/xts/xts_comments-liskov_minematsu .pdf.

[13] Kirat Pal Singh, Shiwani,” An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm “, https :// eprint.iacr.org/ 2016/ 789.pdf.

[14] Vaidyaa M., Dr Shrinivas Deshpandeb ,” Study of Performance Parameters on Distributed File Systems using map reduce “, www.sciencedirect.com ICISP2015), 11-12 December 2015, https://ac.els-cdn.com/S18770509 16000399/1-s2.0-S1877050916000399-main.pdf ?_tid=78 c69a4a-e233-11e7-8cfd-00000aab0f01& acdnat=15134098 15_ d18af66cf2c2e5fa578411397b06ce28

[15] Wei Li, Ming Chen, Mingming Li, “ Information Security Routing Protocol in the WSN”, Published in: 2009 Fifth International Conference on Information Assurance and Security, ISBN: 978-0-7695-3744-3, https://ieeexplore.ieee.org/document/5284242

[16] Sonkar Abhilash., Aggarwal Abhishek, “Enhancement of Security using greedy approach and encryption in Mobile Ad Hoc Network”, Published in: 2017 International Conference on Trends in Electronics and Informatics (ICEI), https://ieeexplore.ieee.org/document/8300887