IMPLEMENTATION AND PERFORMANCE ANALYSIS OF PROPOSED SECURITY FRAMEWORK FOR UIDAI

Arpana Chaturvedi

РЕАЛІЗАЦІЯ ТА АНАЛІЗ ПРОДУКТИВНОСТІ ЗАПРОПОНОВАНИХ ОСНОВ БЕЗПЕКИ ДЛЯ UIDAI

Арпана Чатурведі

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 AESXTS 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*

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 centers 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 vari-

ous 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 five sections. Section 1 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 2 describes the importance and benefits of AES -MR technique highlighting the XTS encryption Mode. Section 3 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 4.

1. 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 us-

ers 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 a vail 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.
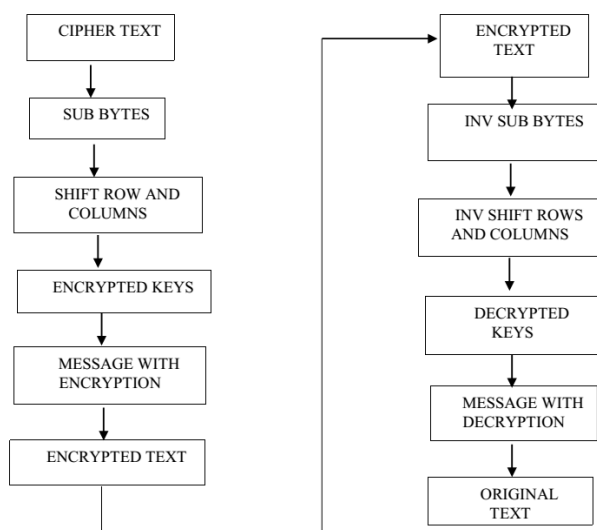

Fig. 1. Encryption and Decryption Process

2. 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.

2.1. 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.
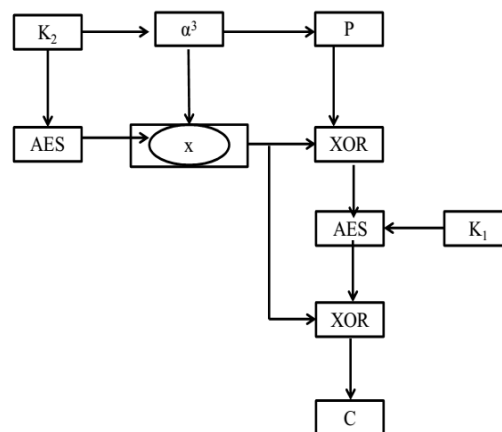

Fig. 2. Operation of AES-XTX Mode with two different keys

2.2. XTS encryption mode

The Electronic Cook Book (ECB) and XTX are used with AES to increases the efficiency 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. 2 [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 ().

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.
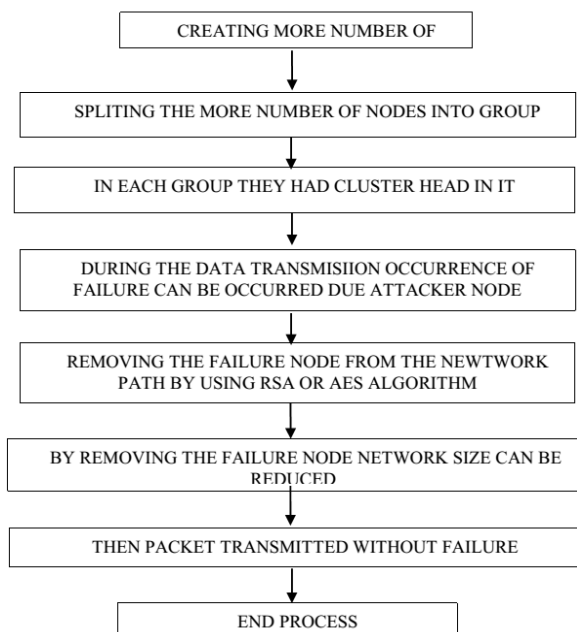

Fig. 3. Flow Chart to show steps used
in Implementation Work

3. 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.

The theoretical analysis and simulation shows the better performance of SAODV by adding proposed se-

curity mechanism to AODV in the routing layer. The steps of implementation work are shown in Fig. 3.

Table 1

Details of Simulation Environment

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,

3.1. 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:

Table 2

Description of Routing Protocol and assigned protocol

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

3.2. Using AES algorithm

In the below shown screenshot (Fig. 4), 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.

Fig. 4. Screenshot of command used to execute
the implementation work

3.3. Output of implementation work

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

i) 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.
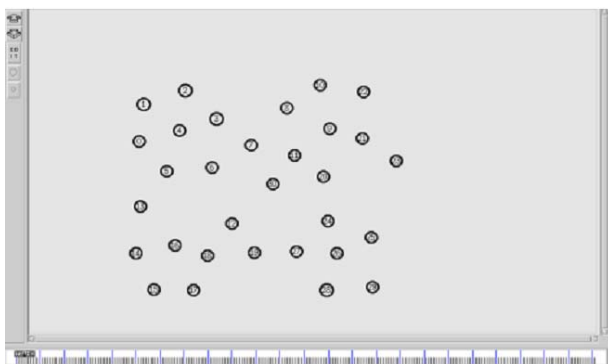

Fig. 5. Screenshot which show Node creation

In the above screenshot (Fig. 5) node creation has been occurred. In this network number of node created is 30.

ii) Allocation of sender and receiver for various nodes

In the below (Fig. 6) screenshot for the formation of group of nodes it had been assign the cluster head with source and destination.
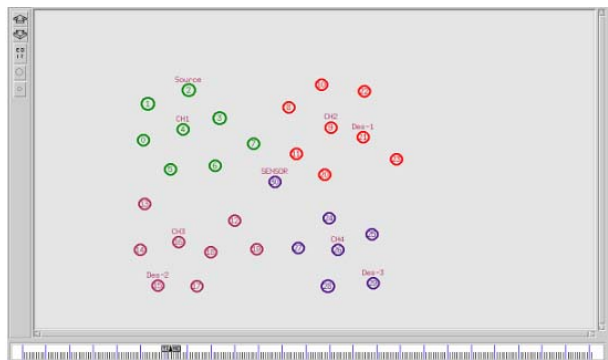

Fig. 6. Assign the cluster head with source and destination

iii) Data transmission

In this graph (Fig. 7) 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.
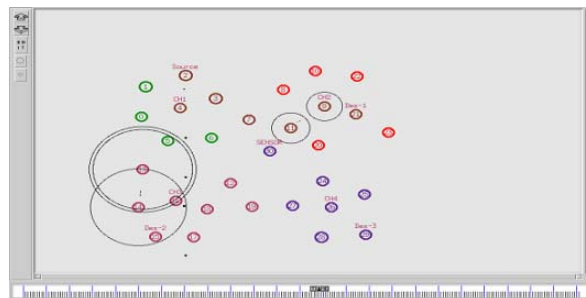

Fig. 7. Selection of Channel by TCP/IP Protocol

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.

iv) Transmission with key exchange

In this graph (Fig. 8) 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.
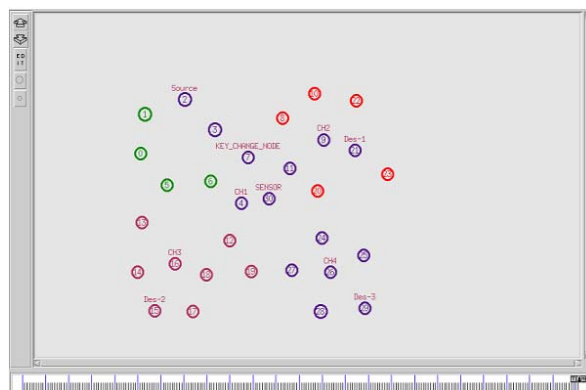

Fig. 8. Transmission of Information with Key Exchange

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.

3.4. Graph Representation

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

i) Drop in data

In this graph (Fig. 9) 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.
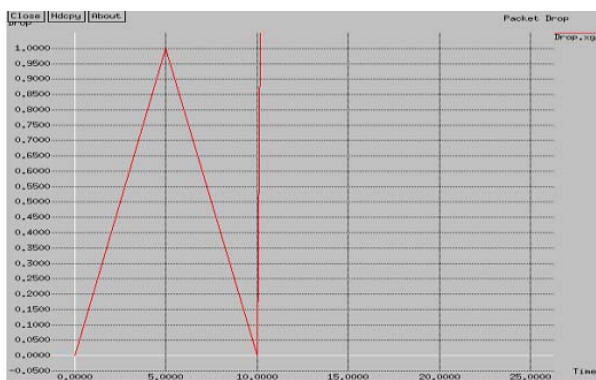
Fig. 9. Packet drop between the Existing
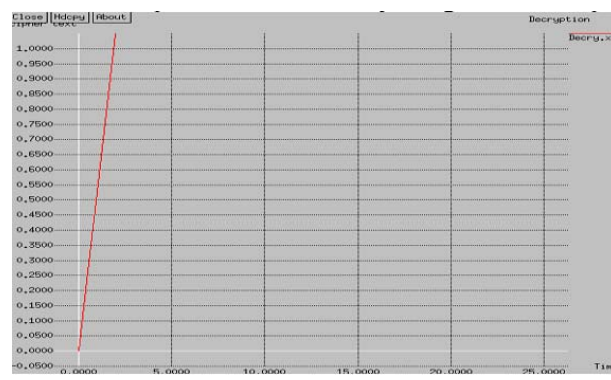and Proposed Method

ii) Data transmission in encryption

In this graph (Fig. 10) 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.
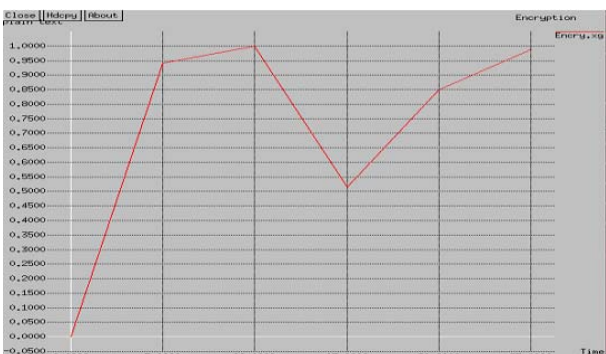

Fig. 10. Filtering of Nodes and Packets

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 the network has been calculated.

iii) Data decryption while data transmission

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

In this graph (Fig. 11.) 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.

iv) Comparison of 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.

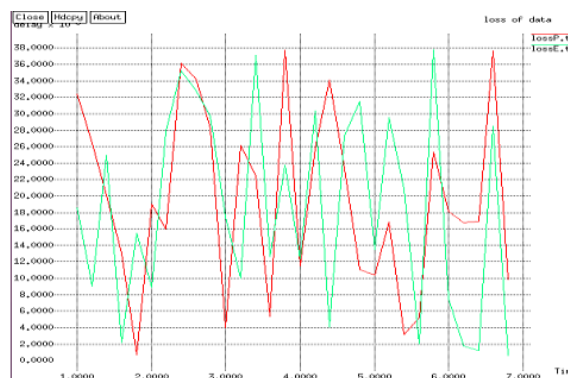Fig. 11. Data Decryption while Transmission of Information

Fig. 12. Loss of Data while Transmission of Information

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

v) 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. 13) 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.
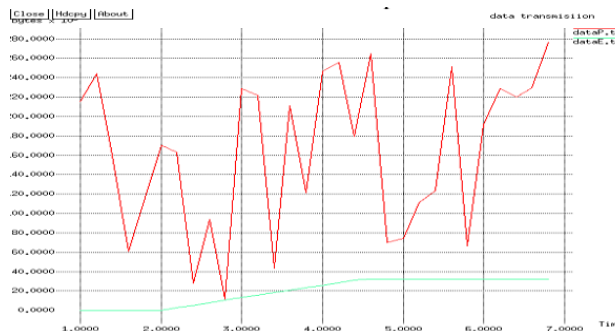

Fig. 13. Increased speed when Data Packets transmitted
through Various Nodes

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

vi) Passing of data with individual key values

In this graph (Fig. 14) 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 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
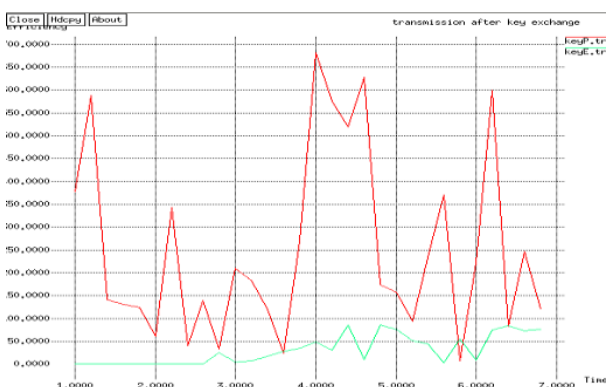

Fig. 14. Comparison of Security implementation in Existing and Proposed Mechanism

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

5. 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 enhance 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 transfers data from nodes towards others. 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 the AES algorithm in WSN and then encryption to expand the demand or of the 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 the government nowadays 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.

R e f e r e n c e s

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%203/U 4903133138.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-andGuidelines/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/c ollected_xts_comments.pdf
5. Public Comments-Modes Development - Block Cipher Techniques, https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Public-Comments-ModesDevelopment,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, Techno-mathematics 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 dmcrypt 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-ciphertechniques/ documents/ bcm/ comm. ents/xts/xts_co mments-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.

Арпана Чатурведі. Реалізація та аналіз продуктивності запропонованих основ безпеки для UIDAI

Розвиток нових технологій, таких як Hadoop, Map Reduce, використовуваних для зберігання, управління і аналізу величезної кількості даних, пов'язаних з WSN (Wireless Sensor Network), збільшує фактор ризику для інформаційної безпеки. При застосуванні їх в різних додатках для уряду, таких як Aadhaar, DigiLocker і т. П., Ймовірність прихованих проблем безпеки збільшується. У цій статті механізм шифрування AESXTS і технологія цифрового підпису використовуються з протоколом маршрутизації AODV (Ad hoc On-Demand Distance Vector), для усунення різних проблем, таких як DoS (відмова в обслуговуванні), прослуховування, імітація, коаксіалізація і т. Д. Теоретичний аналіз проведено з використанням симулятора NS2, а реалізація забезпечує кращу безпеку даних, надійність, передачу та енергоефективність. Представлена реалізація показує, що протокол маршрутизації SAODV (Secure-AODV) при використанні на рівні маршрутизації в цих додатках і системі підвищує його власну здатність до самооборони для боротьби з різними складними прихованими проблемами безпеки.

Ключові слова: *AODV, SAODV, WSN, AES-XTS, UIDAI, DoS.*

Арпана Чатурведи. Реализация и анализ производительности предложенных основ безопасности для UIDAI

Развитие новых технологий, таких как Hadoop, Map Reduce, используемых для хранения, управления и анализа огромного количества данных, связанных с WSN (Wireless Sensor Network), увеличивает фактор риска для информационной безопасности. При применении их в различных приложениях для правительства, таких как Aadhaar, DigiLocker и т. п., вероятность скрытых проблем безопасности увеличивается. В этой статье механизм шифрования AESXTS и технология цифровой подписи используются с протоколом маршрутизации AODV (Ad hoc On-Demand Distance Vector), для устранения различных проблем, таких как DoS (отказ в обслуживании), прослушивание, имитация, коаксиализация и т. д. Теоретический анализ проведен с использованием симулятора NS2, а реализация обеспечивает лучшую безопасность данных, надежность, передачу и энергоэффективность. Представленная реализация показывает, что протокол маршрутизации SAODV (Secure-AODV) при использовании на уровне маршрутизации в этих приложениях и системе повышает его собственную способность к самообороне для борьбы с различными сложными скрытыми проблемами безопасности.

Ключевые слова: *AODV, SAODV, WSN, AES-XTS, UIDAI, DoS.*

Арпана Чатурведі – доцент кафедри інформаційних технологій Йаганатської міжнародної школи менеджменту (JIMS), Нью-Делі, Індія, e-mail: ac240871@gmail.com