International Conference on Science, Engineering
& Management Trends

International Journal of Science,
Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Advanced Encryption Methods for Enhancement in Safety of Big Data

Ms. Sarita, Professor Gaurav Aggarwal

Research Scholar, Faculty of Engineering & Technology, Jagannath University, Delhi NCR, Bahadurgarh.

Abstract- Cloud computing has become a general term. It has been used to the deliver the hosted services. These services are provided over the internet. There are three type of cloud such Public Cloud, Private Cloud, Hybrid Cloud. Several benefits of cloud computing are discussed along with its challenges. Big data is a combination of structured, semi structured and unstructured data. Also we discuss about intrusion detection system.

Keywords- Cloud Computing, Hosted Services, Public Cloud, Private Cloud, Hybrid Cloud, Cloud Services, Internet-based Services

I. INTRODUCTION

In the background of cloud data is transferred rapidly over internet therefore safety of data is always kept in mind. Several customers' data may be affected because they are using the infected cloud for distribution of data. The security challenges counted by cloud computing is described as:

- Integrity of data: Integrity of data consists of situations when some human errors are made, while feeding data. Errors could take place during information is transferred from one system to another. Sometime errors occur due to hardware malfunctions such as crashing hard drives.
- Access Control of Data: Secret information might be illegally stolen in absence of secured data and information access control.
- Theft of Data: Cloud computing applies the external data server for flexible and cost affective tasks. Thus there is an option that from external server theft of information might take place.
- Location of Data: Consumers is unaware from the area where data is stored. Vendor not going to tell consumers where there data has been collected. Cloud Computing is offering a high degree of mobility of information.
- Loss of Data: Loss of data is referred as critical issues in Cloud computing. Unauthorized person might be able to capture data that is shared on cloud if business transaction, banking & research & development ideas are online.
- Issues related to Privacy: Protection of user data has been considered vital with cloud computing. Several servers are external thus vendor must ensure that data is secured from other persons.
- Challanges at User level: it is necessary that the user make sure that possibility of the data loss because of its own action or other user operating at common cloud server.
- Security challanges in supplier level:Cloud is considered best in the case of high security given by vendor to consumer.
- Application that are Infected: Service supplier must have access to server with overall rights to maintain server and to monitor it.

Account or service traffic hijacking

- If login credentials are theft Account could be hacked.
- Insecure API's
- The Application Programming Interface is going to control third party. It also verifies the user.

- Denial of service
- It is done when millions of user request for common service. Hacker takes the advantage in this case.
- Malicious insiders
- It is performed when any one knows our login credentials.
- Misuse of cloud services
- With the help of clouds server, hacker could crack security in less time.

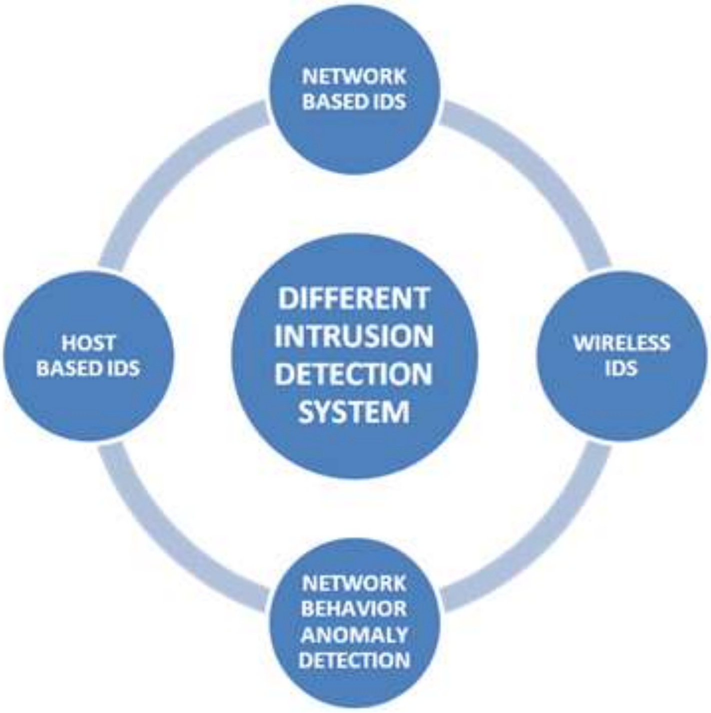
NETWORK BASED IDS
HOST BASED IDS
DIFFERENT INTRUSION DETECTION SYSTEM
WIRELESS IDS
NETWORK BEHAVIOR ANOMALY DETECTION

Figure 1: Different Intrusion Detection System

II. NEED OF INTRUSION DETECTION SYSTEM

This system is required because of the reasons which are discussed here:

- To display definite Content: There are chances that your ports and IP addresses are displayed by Firewalls. These ports and IP addresses are applied in the middle of two hosts. But, at the same time a NIDS could be aired due to which exact content within packets are displayed. It is possible to employ them for the detection of disturbances.
- Examine Data in view of Protocol: In situation where a protocol is assessed by network INTRUSION DETECTION SYSTEM, it examine the load capacity on Transmission Control Protocol and User Datagram Protocol . Unusual actions are identified by sending elements because they understand the manner in which protocols work.
- For authorize and determine Attacks: With the help of this system attacks are authorized and determined. After getting this information one can modify his safety network systems. In addition to this, it is possible that one can put in to operation fresh management tools in a very effective way. It is also examined in order to determine bugs and challenges related to system configuration. After that this metrics could be utilized in assessment of upcoming risk .
- For maintain rules: When this system is used, it is quite easy to satisfy safety rules because this system allows greater visibility across network. It is also possible that one can use his IDS logs in the form of documents for the satisfaction of definitely needs.
- To improve Performance: With the help of this system sensing elements network hardware and hosts are identified. Due to this, data inside the network packets are examined. It can determine

which type of controlling software are used. In comparison to manually working it saves lot of time. IDS make hardware stocks automatic. This will reduce manual requirement. This will bring reduction in the cost which is given to organization employees in the form of salary and the cost which is required for the implementation of IDS.

Des (Data Encryption Standard)

DES is already determined in the form of a symmetric-key algorithm. Its full form is Data Encryption Standard. It is an algorithm used to encrypt the electronic information. DES has short key length of 56 bits. It has been criticized from beginning use of Data Encryption Standard. Due to some issues it presents it as unsecured for several present applications. DES was dominant with the advance technology of cryptography. DES is a symmetric-key block code. NIST made it available to the public. It is a realization of Feistel Cipher. It becomes well known that DES has dependency on the Feistel Cipher. For the specification of DES round function, key plan and some extra treatment like original and concluding variation are compulsory.

Aes (Advanced Encryption Standard)

Nowadays, well known and extensively accepted symmetric encryption algorithm becomes famous in the form of AES algorithm. Full form of AES is Advanced Encryption Standard. The AES algorithm is very fast as compare to the triple DES. It is six time vast as compared to triple DES.

As it has been observed, AES key's dimension becomes very small. Therefore substitute for DES is required. As the computing power is increasing day by day, the AES is vulnerable to deal with exhaustive key search attack. Triple DES has been formulated in order to deal with this drawback. But the speed of it is slow. Alresdy known features of TRIPLE DES As it has been observed, AES key's dimension becomes very small. Therefore substitute for DES is required. As the computing power is increasing day by day, the AES is vulnerable to deal with exhaustive key search attack. Triple DES has been formulated in order to deal with this drawback. But the speed of it is slow. Alresdy known features of

Triple Des

Triple Des applied three separate keys. So that it has been determined secure. The cause is that there are no known attacks that totally crack the security to a point where there is no feasibility nowadays to break Triple DES. Therefore it provides a security margin. But it is still less secure as compare to other standards. The perfect example is AES.

III. CRYPTOGRAPHY

Along with this advantage, it carries its limitation also. The limitation is that it is very complex timplement but computationally it is secure technique. The language in which the human communicates is the human language. It is the form of plain text. It also called clear text. So, messages written in plain text are understandable by all because the message is not codified in this form. Therefore, it must be codified to make sure the security of message. After coding the message will be secure from anyone from who is unauthorized. It will be hidden from who can see the coded message. Nowadays cryptography described almost utterly to encryption. The encryption is a procedure of changing normal data into not understandable form. The text in normal form is called plaintext whereas the text after encryption is called ciphertext. The Decryption is the opposite procedure of encryption. A cipher has been considered an algorithms pair. It is used to do the encryption of text. The detailed operation of a cipher has been monitored by the algorithm. It also monitor in each instance by a "key". A cryptosystem has been determined the arranged record of elements. It consist finite feasible plaintexts, finite feasible ciphertexts. The cryptosystem also includes the finite feasible keys. The encryption and decryption algorithms are also take place in it. These are in contact to each key. The Keys are very essential role. The ciphers lacking variable keys are easily cracked. It will be broken with only the information of the used cipher. In the past, ciphers were applied in direct way for encryption or decryption. It was lacking of additional processes for example authentication or integrity checks. Cryptography has been considered an art of getting the security of data. The security of data is achieved to encode the text and create it in the form of not understandable. The Cryptography is the procedure to study data which have been hiding by encoding.

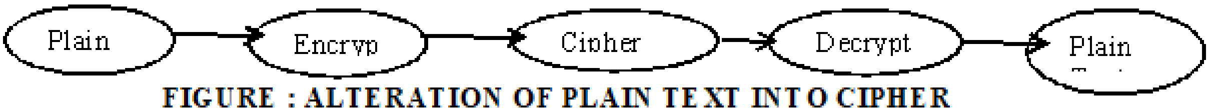

FIGURE : ALTERATION OF PLAIN TEXT INTO CIPHER

A cryptosystem has been studyof encryption & decryption methods & this method could be made effective by hardware devices/program or software code within program. Encryption algorithms are used by cryptosystem, which pronounces how process would be done or execute. Most algorithms use difficult mathematical formulas for protected communication so that third party can't calculate or find password effortlessly.

Result has been applied to plain message

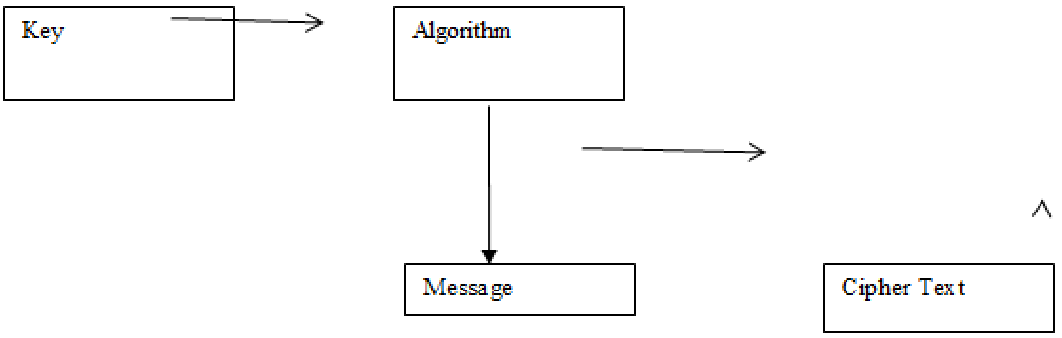

Figure 2: Use Of Key In Cryptosystem

Secret key i.e. long string of bits has been used by frequently encryption methods algorithm to encrypt & decrypt text or content of message, as represented in Figure. The set of mathematical rules or set of events has been called algorithm. There are two kinds of algorithms are used for enciphering & deciphering content of message. Several algorithms are well recognizing publicly. These algorithms aren't secret part of encryption procedure. Method by which the algorithms encryption performs could be retained secret from public, but several of them are publicly recognized & well known. Key has been secret portion for encryption & decryption algorithm.

IV. PROPOSED WORK

Item of the nodes also includes the same elements. It will happens as data packet to broadcast the packets by network.

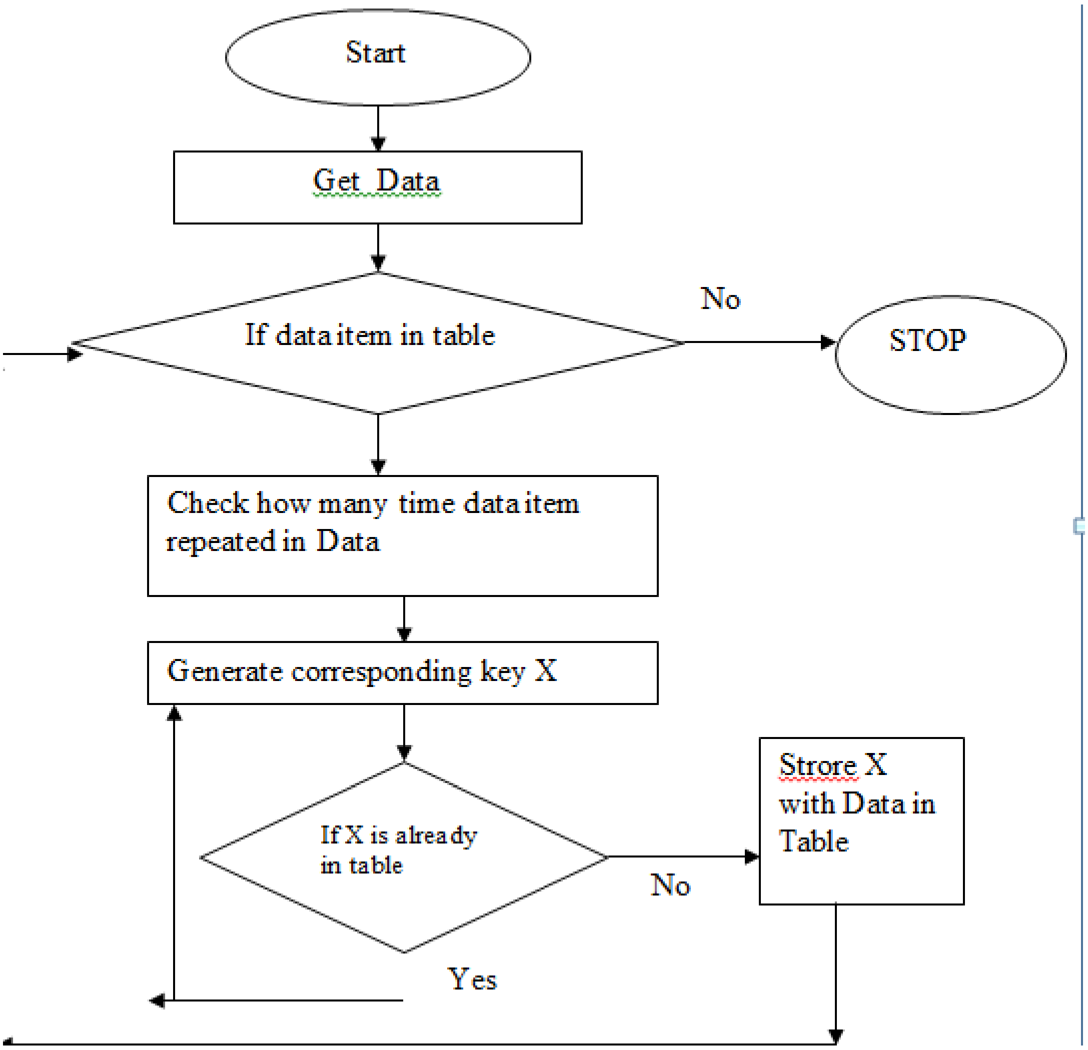
Start
Get Data
If data item in table
No
STOP
Check how many time data item repeated in Data
Generate corresponding key X
If X is already in table
No
Strore X with Data in Table
Yes

Figure 3: Packet Size Reduction Logic

Proposed protocol will use the data packet and control packet. These are two different kinds of the packets. The data packet broadcasts the environmental information to destination. This environmental data includes six components. Here one thing should be noted that buffer sysProposed work has considered the security of cloud. To improve the security of cloud, the concept of IDS method will be used here. It will provide protection as per the requirement. It willalso Iincrease Ithe Ioverall Itime Iperiod Iof Ithe Inetwork. IIt Idecreases Ithe Ipower utilization. Local node network are differentiated into little zones.

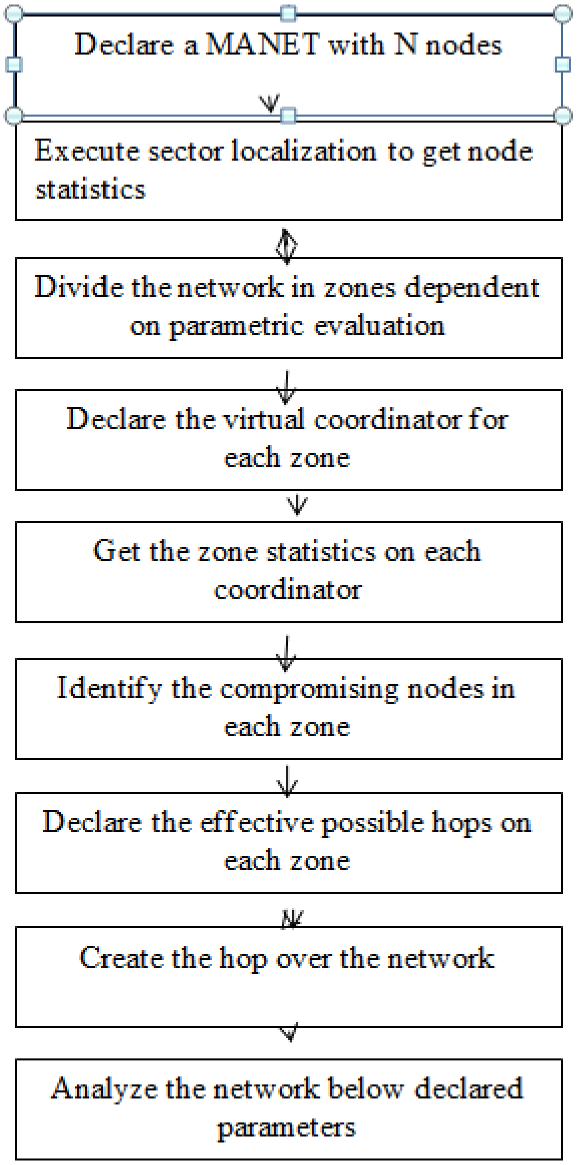
Declare a MANET with N nodes
Execute sector localization to get node statistics
Divide the network in zones dependent on parametric evaluation
Declare the virtual coordinator for each zone
Get the zone statistics on each coordinator
Identify the compromising nodes in each zone
Declare the effective possible hops on each zone
Create the hop over the network
Analyze the network below declared parameters

FIGURE: WORK FLOW

The describe coordinator will include the communication statistics. These communication statistics are of zone nodes. According to routing performance, the effective hop selection are used the virtual coordinator.

V. CONCLUSIONS

Objective of this work is to Establish the Network Environment to test flow of packets, to Develop of packet sender & receiver module, to testing transmission delay in packet transmission, to Test the processing delay during packet transmission, to test the queuing delay of network packet, to Test the propagation delay at time of data transmission, to Develop the algorithm using java based socket programming to transfer packet from sender to receiver in minimum time, to develop better encryption model in order to resolve the hacking issues. In this thesis discussion will be made on the researches based on how we secure big data in cloud computing. Discussion of security algorithm has been made that are capable to secure data.

Reduction of packet size using packet reduction logic leads to less space and time consumption. Mat lab based simulation representing the working comparative analysis of time taken between tradition and proposed work after load balancing will conclude that proposed model will take less time. The main concentration of this research is towards the strategies of energy-efficient resource arrangement and security of data over cloud.

REFERENCES

1. Amandeep Kaur, Dr. Amardeep Singh (2014) A Review on Security Attacks in Mobile Ad-hoc Networks, International Journal of Science & Research, Volume 3 Issue 5, might 2024
2. .Md. Waliullah, (2014) Wireless LAN Security Threats & Vulnerabilities, International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2022
3. .Jhilam Biswas, Ashutosh (2014) An Insight in to Network Traffic Analysis using Packet Sniffer, International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, might 2021
4. .Blessy Rajra, A J Deepa (2015) A Survey on Network Security Attacks & Prevention Mechanism, Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2020
5. .Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. , Issue. 5, May 2015, pg.786 – 791.
6. .ManpreetKaur, Hardeep Singh (2015) A review of cloud computing security issues International Journal of Advances in Engineering and Technology, June, 2015.
7. .Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil (2015) Cloud Computing – A market Perspective and Research Directions I.J. Information Technology and Computer Science, 2018
8. .Raj Kumar(2023) Research on Cloud Computing Security Threats using Data Transmission International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015 ISSN: 2277 128X
9. .BurhanUl Islam Khan, Rashidah F. Olanrewaju, AsifaMehraj Baba(2015) Secure-Split-Merge Data Distribution in Cloud Infrastructure, IEEE Conference on Open Systems (ICOS), August 24-26, 2017
10. .Jianghong Wei, Wenfen Liu, Xuexian Hu(2015) Secure Data Sharing in Cloud Computing Using
11. .AL-MuseelemWaleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.
12. .Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.
13. Babitha. M. P, K.R. RemeshBabu, "Secure Cloud Storage Using AES Encryption", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), ©2016 IEEE.
14. .SakshiChhabra, Ashutosh Kumar Singh(2016) Dynamic Data Leakage Detection model based approach for Map Reduce Computational Security in Cloud,
15. G.M.Nasira, Thangamani(2023) Securing Cloud Database By Data Fusing Technique (DFT) Using Cloud Storage Controller (CSC), 2016 IEEE International Conference on Advances in Computer Applications (ICACA)
16. .Aaron Zimba, Chen Hongsong, Wang Zhaoshun(2016) An Integrated State Transition-Boolean Logic Model for Security Analysis in Cloud Computing 2016 First IEEE International Conference on Computer Communication and Internet
17. .Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. Kailash D. Kharat,(2017) "Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques"
18. .P. R. Merla and Y. Liang, "Data analysis using hadoop MapReduce environment," Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017, vol. 2018–Janua, pp. 4783–4785, 2018.