Enhancement of Big Data Security in Cloud Environment

Anshi Singh, Anjani Rai,

Anshi Singh, Anjani Rai,
Department of Computer Engineering and Applications,
GLA UNIVERSITY, MATHURA.
Department of Computer Engineering and Applications,
GLA UNIVERSITY, MATHURA.
E- Mail: anshy.singh@gla.ac.in

ABSTRACT

In this research, the advanced encryption mechanism is discussed to secure big data in cloud computing. The services of Cloud computing are used on broad level because these services are Platform independent. Cloud computing eliminates the need to set specific software on system of user. To improve the security of cloud, the concept of Advanced Encryption Standard (AES) with Intrusion Detection System (IDS) method is integrated here. It is capable to offer the protection according to demands. It also enlarges the overall time period of the network. It is made to decrease the power utilization by the node. For optimum the local node network is differentiated into little zones. In addition, the algorithm for encoding is mentioned which is used to make encryption with Advanced Encryption Standard (AES).

Keywords: Cloud Computing, Encryption Mechanisms, Cryptography, AES and IDS.

INTRODUCTION

Availability of computer system resources according to need of user, is known as Cloud computing. Especially, it is the availability of data storage and computing power. In Cloud Computing, the user of cloud services is not required to do direct active management. The term “Cloud Computing” basically stands for data centres that are easy to use by many users via Internet [23]. Cloud Computing is the easy access of hardware and software in order to complete a particular task via internet or may be other network. Using the concept of Cloud Computing, users are able to get access of files and applications situates on Cloud via Internet Connection. Google's Gmail can be discussed as an example of Cloud based Apps [24].

In Cloud Computing, Information and data of user has been stored on physical or virtual servers. Cloud computing providers maintain and control these servers. As an example, Amazon Company and also their AWS product can be discussed [25]. One can use cloud based services for personal and business purpose. One can store and access his information or data on the 'cloud' through Internet. Three main kinds of cloud computing are there. First type is Software-as-a-service (SaaS). It is used to create web-enable apps. Second is infrastructure-as-a-service (IaaS). it is required to access the storage and computing power[26]. Third is platform-as-a-service (PaaS). In this type, the tools are provided to developer for creating hosting of Web apps [27].

CHALLENGES WITH CLOUD SERVICES

As there are several benefits of Cloud Services, several security challenges are also with these services. These are also considered here:

a. **Data Stealing:** In Cloud computing, external data server are used in order to perform elastic and cost affective jobs. Therefore, there are chances of data stealing from external server.
b. **Insecure API’s:** The Application Programming Interface (API) is controlled by any third party. It makes verification of user. So it is possible that there may be some issues with Sensitive Data.
c. **Denial of service:** It is a type of attack on Data or information. This type of attackers takes place when user request for common service in millions.
d. **Integrity of data:** Integrity of data stands for situations in which user make some errors in feeding the data. In other case, some errors may be occurred at the time of information travelling from one system to another. There may be situation of Crashing of Hard Drives and errors occur.
e. **Access Control of Data:** In the absence of Secret information access control system, there is the probability of illegal access of data.
f. **Malicious insiders:** Malicious attackers can attack on an account knowing login credentials about an account.
g. **Misuse of cloud services:** Hacker or attacker can crack security or protection in less time with the help of clouds server.

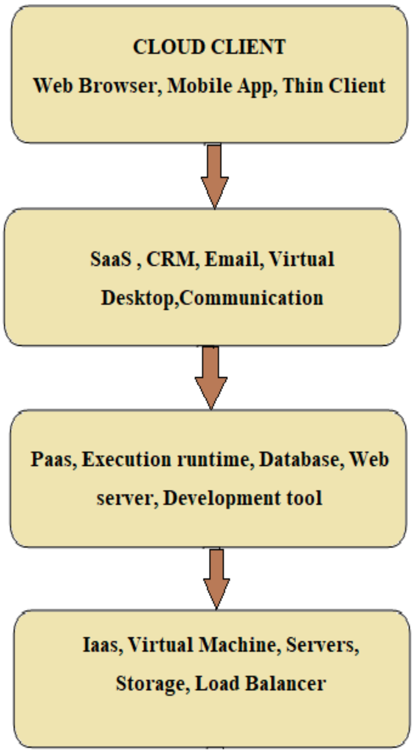
CLOUD CLIENT
Web Browser, Mobile App, Thin Client
SaaS , CRM, Email, Virtual Desktop,Communication
Paas, Execution runtime, Database, Web server, Development tool
Iaas, Virtual Machine, Servers, Storage, Load Balancer

Fig 1: Cloud Computing Layers.

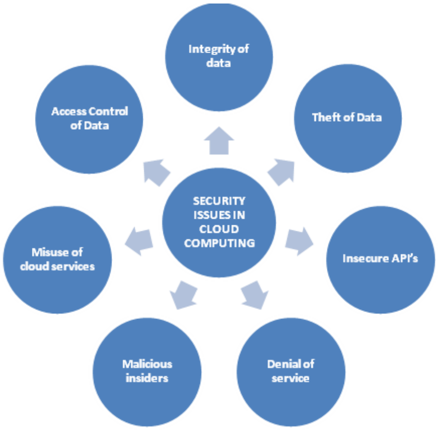

Fig 2: Security Issues with Cloud Computing

BIG DATA

Big data stands for huge data sets which are analyzed in order to understand the patterns, trends etc. specially; it is used to analyze the behaviour of human beings. In order to deal with Big Data, old and new technologies are merged. This integrated mechanism allows companies or organizations to obtain actionable perception. At all, it can be said that different techniques are required to manage big data which consist of huge volume of unrelated data. As the web based big data creation is increasing day by day. So it is essential to propose best techniques or mechanisms.

LITERATURE REVIEW

There are several papers and article which are proposed to provide knowledge about Cloud Computing and about this technology. Some of researches are reviewed here:

In 2020, Amalarethinam,[1] studied on Cloud Security Algorithms. Since all the clients store their information in the cloud, there is a need of genuine fixation on Data Security. This overview shows the different Cloud Security Algorithms and recommended the requirement for new Enhanced Algorithms considering different Security parameters including cost and speed as main considerations.

In 2020, Sinchana, [2] surveyed the challenges with Cloud Computing Security. The principle point here is to give security to the information by ensuring it by unapproved clients during the hour of data transmission. Distinctive encoding strategies are used for this purpose. This article also presented ongoing procedures and algorithms are proposed by them in order to make sure security of cloud information.

In 2019, Herardian, et al[3] proposed Soft Underbelly related to security of Cloud services. In spite of their earnest, attempts to build up appropriate security arrangements and controls. Except if there is specialized requirement and provable responsibility, building up security arrangements and performing consistence related reviews serve just to cultivate the dream of control.

In 2018, R. Merla et al[4] did Data evaluation utilizing hadoopMapReduce. This research work examines the YouTube information utilizing HadoopMapReduce model. Hadoop multi hub bunch is arrangement on private cloud called AWS (Amazon Web Services). The video measurements got from the API are put away into the HDFS (Hadoop Distributed File System) and the information preparing is finished by the MapReduce framework.

In 2017, Suraj R. Pardeshi,[5] upgraded Information Security in Cloud Computing Environment Using Cryptographic Techniques. Although they have existing procedures symmetric and assymetric key cryptography techniques, however there exists a security concern. A short depiction of proposed system is characterized which employments the irregular blend of open and private keys.

In 2016, Aaron Zimba,[6] proposed an Integrated State Transition-Boolean Logic Model. This model was proposed to provide the security evaluation on Cloud Computing. In any case, security prerequisites do change with time and this along these lines requires a nonstop procedure of assessing the security status of the cloud framework. This article proposes a model of breaking down the security status of the cloud framework. In their model, they have provided secrecy, uprightness and accessibility.

In 2016 Dr.G.M.Nasiraet_al[7] presented a Data combine approach by utilizing Cloud Storage Controller. it was made for the assurance of Cloud related record. They presented an information combined approach with the Cloud Storage Controller. It was used for the insurance of data which is gathered cloud records from notable assaults. It is generally incredible.

In 2016 SakshiChhabra,[8] they proposed the idea Map Reduce Computational Security in Cloud. Technique is put together by them which are useful in the improvement of working effectively. Notwithstanding this they make made sure about data in Map Reduce calculation circumstance. Their fundamental goal is to accomplish data assurance and to fend off data outpouring.

In 2016, Babitha. M. P [9] composed an exploration that tended to different data security and disengagement challenges in encompassing of distributed computing. They set forward a plan to gracefully offices for security like accreditation support and tact. In such plans, data is encoded by utilizing AES. After that this data is transferred on a cloud.

In 2016 Nidal Hassan Hussein [10] composed a paper. In such research, an across the board investigation of introduced writing for distributed computing security concerns and strategy for their goals is submitted.

In 2016 AL-MuseelemWaleed, Li Chunlin [11] highlighted the concerns related with security and segregation is uncovered in context of distributed computing. One of the significant expectations behind this work is to highlight the concerns related with security and segregation in distributed computing. For this purpose, the Ubuntu Enterprise Cloud can be used.

In 2015, A. Bhardwaj, et al[12] wrote on BigData with Hadoop. From this research's result, it has been discovered that CPU execution time to complete the employments decline as the quantity of Data Nodes in HDInsight group increments. These results demonstrate the great reaction time with increment in execution just as more consumer loyalty.

In 2015 Jianghong Wei, Wenfen Liu, Xuexian Hu [13] perceived that if circulation of data is done securely in Cloud Computing it gives an adaptable and helpful plan for designation of information

In 2015 BurhanUl Islam Khan [14] discussed on safe Data Distribution within Cloud environment. They have recognized that ensured isolate consolidate records course in Cloud Infrastructure. The exploration essentially focuses on security worries of paid shoppers so as to satisfy their Service Level Agreement for gathering office on cloud.

In 2015 Raj Kumar [15] researched on Challenges related to security of Cloud Computing Security. In this research work, Data Transmission technique is determined. This work recognized that one of the pervasive deterrents in endorsement of distributed computing is wellbeing. In Software engineering provides us Distributed computing based some facilities and web apps that are available through Internet.

In 2015 Amol C. Adamuthe [16] provided a market viewpoint and Research Directions on Cloud Computing. Great consolation from governments, mass PC program and types of gear organizations, researcher and shoppers is appeared for Cloud based services.

In 2015 ManpreetKaur [17] identified the security issues of Distributed Computing. Presently a day, it is viewed as that Distributed computing is modern information which is widely utilized globally. Presently a days of cloud based services are used in schools, universities notwithstanding association circle. By giving conviction it is conceivable to overcome the challenges identified with security since it makes relationship rapidly and securely.

In 2015 Karun Handa [18] portrayed a view of Cloud Computing. It is very easy to accumulate assets which are available. Without distributed computing, a lot of cash is contributed. Besides availability of assets should be possible effectively in light of the fact that everyone could get to data via web services.

In 2015, BlessyRajra[19] presented a security structure by utilizing Location subordinate assistance (LBS) with the assistance of which it is anything but difficult to pick up data .It functions as a strengthening segment in confirmation process. A buyer is treated as real shopper in the event that he contains official grant in area inside association.

In 2014 JhilamBiswas [20] presented Network Traffic Evaluation. In this work, for Packet Sniffer is also considered. They discussed that Wire shark is one of Network packet Analyzer. It is basic thing that Communication framework official must think about the noteworthiness of utilizing this type of hardware.

In 2014 Md. Waliullah [21] it is assumed by them that making sure about remote framework or system is a suffering strategy. Convincingly at present there isn't an individual security strategy which is considered as accurate and can be access easily. These security systems are enabled to effortlessly move and can be access by everybody.

In 2014 AmandeepKaur [22] discussed about transmission system for example MANETs. These systems are more susceptible to countless attacks. The Reason is that these systems have energetic construction and have not federal management. The researcher of this work considered the security challenges related to cloud computing services.

PROPOSED MODEL

In this proposed model, data packet and control packet are considered. Two separate types of packets are there. The data packet is responsible to broadcast the selected data to its destination.

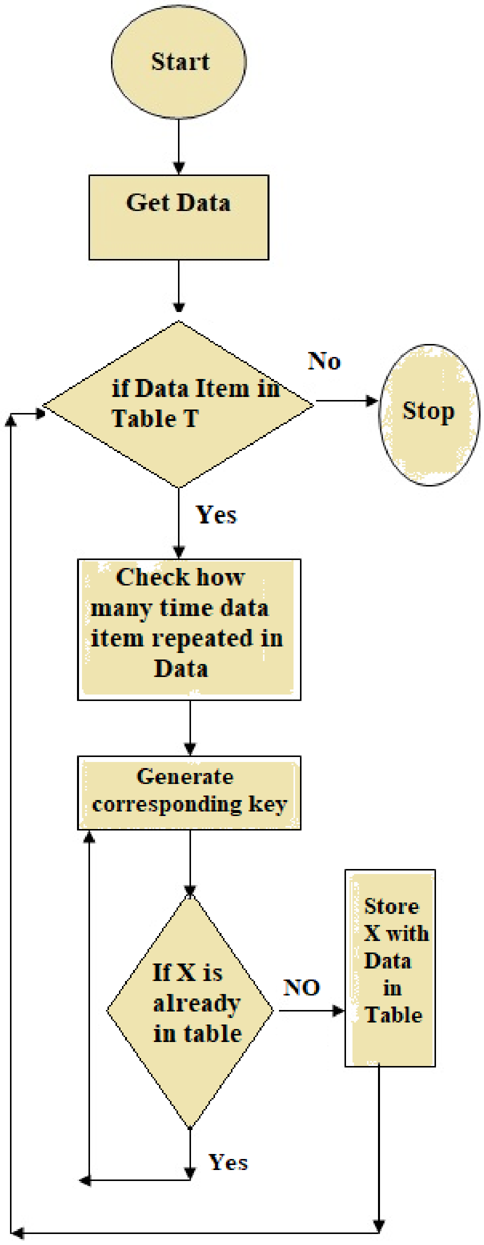
Start
Get Data
if Data Item in Table T
No
Stop
Yes
Check how many time data item repeated in Data
Generate corresponding key
If X is already in table
NO
Store X with Data in Table
Yes

Fig.3: Process Flow of Proposed Model

There are six components that are considered in this data packet. It is a considerable thing that these same elements are also determined in a buffer system.

CRYPTOGRAPHY (ENCRYPTION AND DECRYPTION OF DATA)

Cryptography has been known as an art used to secure the data transmission over internet. There are several Cryptography techniques and codes which are used to make secure data transmission between sender and intended recipient over internet. When the electronic data is transmitted, cryptography techniques are applied for encryption and decryption of data that may be email or other Web Based app. In Modern cryptography, complicated mathematical equations or algorithms are used. Along with this, secret keys are also determined for encryption and decryption of data. At present scenario, cryptography stands for secrecy as well as integrity of Web based Apps or their data.

CONCLUSION

In the proposed protocol, the data packet and control packet are considered. To improve the security of cloud, the concept of IDS method is used here. It is capable to offer the protection according to demands. At all, it can be said that the proposed encryption mechanism with the IDS technique is efficient to secure big data in cloud computing. In the research work, According to routing performance, the effective hop selection is used to the virtual coordinator.

FUTURE SCOPE

This paper would be beneficial as it considers the security of big data sets over cloud. It provides the integration of Advanced Encryption System (AES) with Intrusion Detection System (IDS) technique for security of Cloud Based Services. This proposed model is capable to offer security according to demands. It is able to enlarge the complete life time of network. It is possible as selected Nodes consume less power. Local node is optimized to divide the network within smaller zones. This model would be helpful for secure big data on Cloud.

REFERENCE

1. Amalarethinam, George &Leena, H.M. (2020). CLOUD SECURITY ALGORITHMS - A SURVEY.
2. Sinchana, M. &Savithramma, R. (2020). Survey on Cloud Computing Security. 10.1007/978-981-15-2043-3_1.
3. Herardian, Ron. (2019).The Soft Underbelly of Cloud Security. IEEE Security & Privacy. 17. 90-93. 10.1109/MSEC.2019.2904112.
4. P. R. Merla and Y. Liang, “Data analysis using hadoopMapReduce environment,” Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017, vol. 2018–Janua, pp. 4783–4785, 2018.
5. Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. Kailash D. Kharat,(2017) “Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques”
6. 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
7. G.M.Nasira, Thangamani(2016) Securing Cloud Database By Data Fusing Technique (DFT) Using Cloud Storage Controller (CSC), 2016 IEEE International Conference on Advances in Computer Applications (ICACA)
8. SakshiChhabra, Ashutosh Kumar Singh(2016) Dynamic Data Leakage Detection model based approach for Map Reduce Computational Security in Cloud,
9. Babitha. M. P, K.R. RemeshBabu, “Secure Cloud Storage Using AES Encryption”, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), ©2016 IEEE.

10. 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.
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. A. Bhardwaj, V. K. Singh, Vanraj, and Y. Narayan, “Analyzing BigData with Hadoop cluster in HDInsight azure Cloud,” 12th IEEE Int. Conf. Electron. Energy, Environ. 2015
13. Jianghong Wei, Wenfen Liu, Xuexian Hu(2015) Secure Data Sharing in Cloud Computing Using
14. 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, 2015
15. Raj Kumar(2015) 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
16. 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, 2015
17. ManpreetKaur, Hardeep Singh (2015) A review of cloud computing security issues International Journal of Advances in Engineering and Technology, June, 2015.
18. Karun Handa, Uma Singh, “Data Security in Cloud Computing using Encryption and Steganography”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791.
19. BlessyRajra, A J Deepa (2015) A Survey on Network Security Attacks & Prevention Mechanism, Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2015
20. JhilamBiswas, Ashutosh (2014) An Insight in to Network Traffic Analysis using Packet Sniffer, International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, might 2014
21. Md. Waliullah, (2014) Wireless LAN Security Threats & Vulnerabilities, International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014
22. AmandeepKaur, Dr.Amardeep Singh (2014) A Review on Security Attacks in Mobile Ad-hoc Networks, International Journal of Science & Research, Volume 3 Issue 5, might 2014
23. Kumar, R., Bhardwaj, D. “An improved moth-flame optimization algorithm based clustering algorithm for VANETs” Test Engineering and Management 82(1-2), pp. 27-35, 2020.
24. Bhardwaj, D., Kant, K., Chauhan, D.S. “QoS-aware routing protocol using adaptive retransmission of distorted descriptions in MDC for MANETs” International Journal of Ad Hoc and Ubiquitous Computing 28(1), pp. 55-67, 2018.
25. Kumar, R., Bhardwaj, D., Mishra, M.K. “Enhance the Lifespan of Underwater Sensor Network through Energy Efficient Hybrid Data Communication Scheme” International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control, PARC 2020 9087026, pp. 355-359, 2020.
26. Varun K L Srivastava, N. Chandra Sekhar Reddy, Dr. Anubha Shrivastava, "An Effective Code Metrics for Evaluation of Protected Parameters in Database Applications", International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.1.3, 2019. doi.org/10.30534/ijatcse/2019/1681.32019
27. Bhardwaj, D., Jain, S.K., Singh, M.P. “Estimation of network reliability for a fully connected network with unreliable nodes and unreliable edges using neuro optimization” International Journal of Engineering, Transactions A: Basics 2(4), pp. 317-332, 2009.