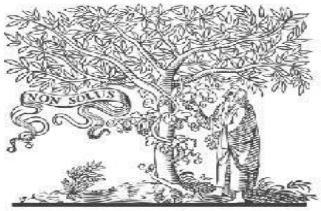
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 11th Aug 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/71

Title **Security Improvement for Big Data in the Cloud**

Volume 12, ISSUE 08, Pages: 482-488

Paper Authors **Dr.Sateesh Nagavarapu, N.Pavan, Kavya Kundeti,Praneeth Emmadishetty**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Security Improvement for Big Data in the Cloud

[1]Dr.Sateesh Nagavarapu, [2]N.Pavan, [3]Kavya Kundeti,[4]Praneeth Emmadishetty
[1] Professor, [2]Assistant Professor, [3,4]Student,
[1,2,3,4] Computer Science & Engineering
[1,2,3,4] Malla Reddy Institute of Technology, Maisammaguda, Hyderabad-500100
[1]sateeshnagavarapu@gmail.com,
[2]npavan26@gmail.com,
[3]kundetikavya@gmail.com,
[4]praneeth.emmadishetty@gmail.com.

ABSTRACT
Big data security in cloud computing is explored together with the sophisticated encryption technology. Because they are platform neutral, cloud computing services are utilized widely. The necessity to install particular software on a user's device is gone thanks to cloud computing. The idea of Advanced Encryption Standard (AES) and Intrusion Detection System (IDS) approach is merged here to increase the security of cloud. It has the ability to provide protection in accordance with needs. Moreover, the network's overall temporal span is extended. It is designed to reduce the node's power consumption. The local node network is divided into small zones for best performance. Moreover, the encoding algorithm used by the Advanced Encryption Standard for encryption is explained (AES).

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

1. INTRODUCTION

Cloud computing is the access of computer system services based on user demand. The accessibility of disk space and computer power is very essential. The customer of cloud services is not needed to do direct active management with cloud computing. Storage systems which are simple for numerous users to access via the Internet are essentially what the phrase "cloud computing" refers to [15]. Cloud computing is the simple access to both software and hardware for the purpose of finishing a certain task over the internet or possibly another network. Users can access files and programmes located on the cloud using the notion of cloud computing and an internet connection. One example of a cloud-based app is Gmail from Google [16]. Information and data of user are stored on real or virtual servers in cloud computing. These servers are controlled and maintained by cloud computing companies. One example is the Amazon Corporation and their AWS product [17]. Both personal and professional uses of cloud-based services are possible. Through the Internet, one can save and access their data or information in the "cloud." There are three primary categories of cloud computing. A good example is software as a service (SaaS). It is utilized to make web-enabled applications.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Infrastructure as a Service comes in second (IaaS). To access the storage and computing power, it is necessary [18]. Platform-as-a-Service comes in third (PaaS). For this kind of hosting, developers are given the necessary tools [19].

CLOUD COMPUTING

It's storage or accessing your data or information and programs over a internet rather than in your hard disk drive or personal computer.

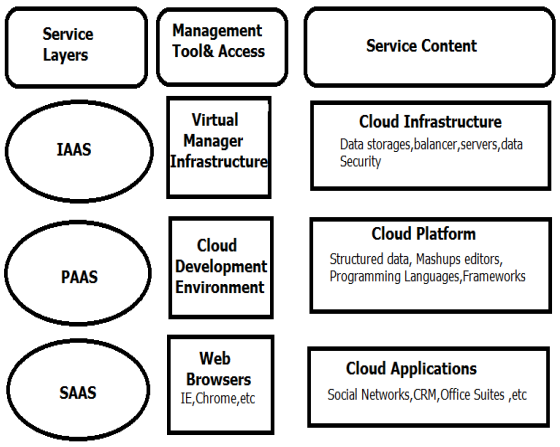


Fig:1. Service Layers of Cloud Computing.

2. SECURITY CHALLENGES WITH CLOUD SERVICES

In addition to their many advantages, cloud services can provide a number of security risks. They are also taken into account here:

a. Data Stealing: With cloud computing, external data servers are employed to carry out flexible and affordable tasks. There is therefore a possibility of data theft from an external server.

b. Unsecure APIs: Any third party has authority over the Application Programming Interface (API). It does user verification. As a result, there could be some problems with sensitive data.

c. Denial of service: A type of attack on data or information. Attackers of this kind occur when millions of users request a shared service. In addition to their many advantages, cloud services can provide a number of security risks. They are also taken into account here:

d. Data theft: With cloud computing, external data servers are employed to carry out flexible and affordable tasks. There is therefore a possibility of data theft from an external server.

e. Misuse of cloud services: A type of attack on data or information is called a denial of service. Attackers of this kind occur when millions of users request a shared service.

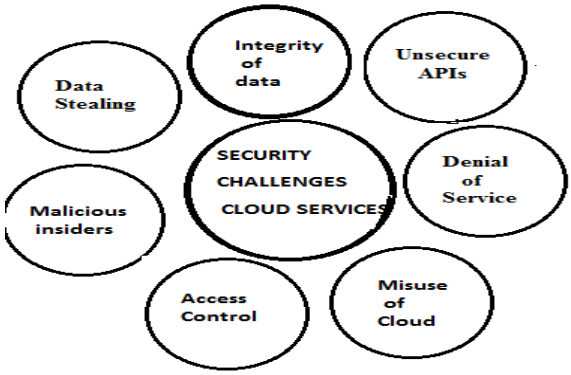


Fig.2 Security challenges cloud services

BIG DATA

Big data refers to enormous data sets that are studied to determine patterns, trends, and other things and it is particularly utilized to study how people behave. An amalgamation of new and ancient technology is used to handle Big Data. Companies or organizations can get actionable perspective thanks to this integrated method. It is true that big data, which consists of a sizable volume of unconnected data, requires the use of a variety of methodologies. As the

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

production of big data on the web climb every day. So, it is crucial to suggest the appropriate methods or strategies.

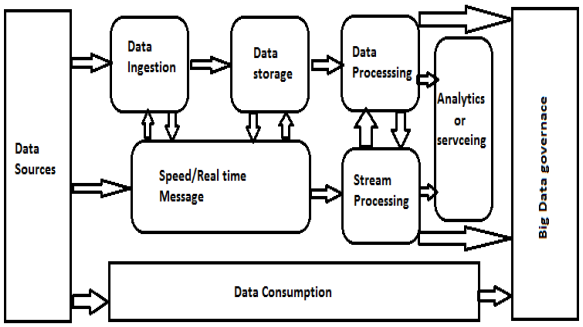


Fig:3. Big Data architecture

3. LITERATURE REVIEW

To educate people on cloud computing and its importance on this technology, a number of papers and articles have been planned. Below is a review of a few studies:

In year 2020 Amalarethinam [1] cloud security algorithms were researched. As every client stores their data on the cloud, there needs to be a sincere focus on data security. This overview demonstrates the various Cloud Security Algorithms and suggests the need for new, enhanced algorithms while taking many security aspects, including speed and cost, into account.

In year2020, Sinchana, [2] the difficulties with cloud computing security were surveyed. The main goal here is to secure the data by preventing access from unauthorized clients at the time of data transmission. For this, many encoding techniques are employed. This article also discussed current practices and methods that are suggested by them to ensure the security of cloud data.

In 2019, Herardian, et al[3] suggested Soft Security-related underbelly of cloud services. Despite their best efforts to establish suitable security measures and controls. Building up security measures and carrying out consistency-related evaluations only serve to foster the dream of control unless there is a specific requirement and demonstrable accountability.

In 2018, R. Merla et al[4] Using Hadoop MapReduce, evaluate your data. With the use of the Hadoop Map Reduce paradigm, the YouTube data is examined in this study project. Multi-hub Hadoop configuration on the AWS private cloud (Amazon Web Services). The HDFS (Hadoop Distributed File System) is used to store the video measurements obtained via the API, and the MapReduce framework.

In 2017, Suraj R. Pardeshi,[5] using improved cryptographic techniques for information security in a cloud computing environment. Despite the fact that symmetric and asymetric key cryptography procedures already exist, there is a security risk. A brief description of the proposed system is given, which uses an unusual combination of open and private keys.

In 2017,Sateesh Nagavarapu,[6].We identified a potential internal security risk from cloud suppliers who offer data mining services in this investigation. The IR encryption technique was suggested as a solution to the security problem. To protect the outcomes of the data mining, we have installed IR. The IR protocol aids the system in protecting the outcomes of data mining. To prevent the information from being seen from the server side, the original IR protocol

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

calls for extracting the complete dataset; however, we decided to use a more effective IR methodology in this study

In 2016, Aaron Zimba,[7] Integrated State Transition-Boolean Logic Model was suggested. This approach was put up to offer an assessment of cloud computing's security. Yet, security requirements do evolve over time, necessitating a continuous process of evaluating the security state of the cloud infrastructure. This article suggests a paradigm for decomposing the cloud framework's security state. They have offered accessibility, uprightness, and confidentiality in their model.

In 2016 SakshiChhabra,[8] Map Reduce Computational Security on the Cloud was their suggested solution. They develop techniques that help with the enhancement of working effectively. Despite this, they ensure that the data is accurate while using Map Reduce. Their main objectives are to protect against data outflow and achieve data assurance.

In 2016, Babitha. M. P [9] written a study that focused on several data security and disengagement issues in the context of distributed computing. They put up a plan to secure offices with elegance, tact, and support for accreditation. Data is encoded using AES in such plans. Then, the data is uploaded to a cloud Openness and uprightness.

In 2016 AL-MuseelemWaleed, Li Chunlin [10] In the context of distributed computing, problems like security and segregation are underlined. One of the main goals of this work is to draw attention to the issues with security and segregation in distributed computing. The Ubuntu Enterprise Cloud can be used.

In 2015, A. Bhardwaj, et al[11] he wrote about Hadoop and BigData. According to the findings of this study, CPU execution time to complete the jobs decreases as the number of Data Nodes in the HDInsight group grows. These results show a superior reaction time along with an increase in execution and more customer loyalty.

4. PROPOSED MODEL

Data packets and control packets are taken into account in this proposed paradigm. There are two different sorts of packets. The chosen data must be transmitted to the destination by the data packet.

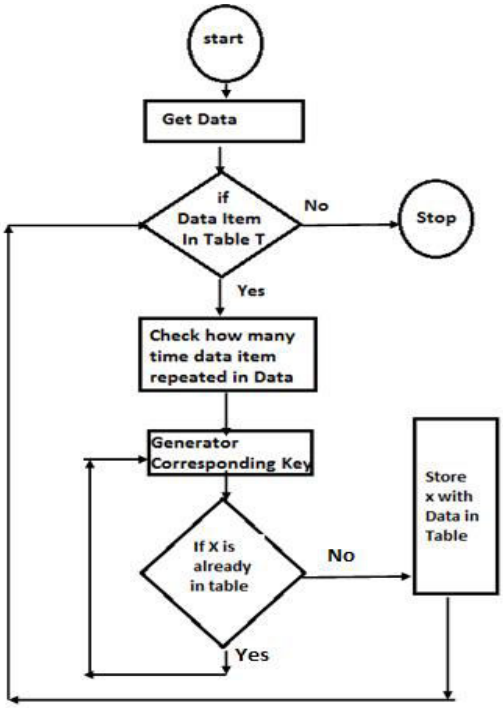


Fig.4.Process Flow of Proposed Model

Data transmission via the internet is known to be securing thanks to the art of cryptography. To ensure safe data transfer between the sender and the intended recipient over the internet, many cryptography techniques and codes are utilized. Cryptography techniques are used to encrypt and decrypt data that may be sent over email or another Web-based application when it is delivered electronically. Complex mathematical formulas or algorithms are used in modern cryptography. Secret keys are also established in conjunction with this for the encryption and decryption of data. In the current situation, cryptography represents the confidentiality and integrity of web-based applications or their data.

5. CONCLUSION

The data packet and the control packet are taken into consideration in the proposed protocol. The idea of IDS approach is applied here to increase cloud security. It has the ability to provide protection in accordance with needs. In any case, it can be said that the suggested IDS technique and encryption mechanism are effective in protecting huge data in cloud computing. According to routing performance, the virtual coordinator is employed in the research work with an effective hop selection.

6. FUTURE SCOPE

Given that this paper takes cloud-based huge data sets' security into account, it might be useful. For the security of cloud-based services, it offers the combination of Advanced Encryption System (AES) and Intrusion Detection System (IDS) technology. This suggested model has the capacity to provide security in accordance with needs. It has the ability to extend the network's entire life. As some Nodes use less power, it is feasible. The local node is designed to segment the network into more manageable zones. Using this strategy might help safeguard huge data in the cloud.

7. 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. 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.

16. 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.

17. 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.

18. 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

19. 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.

20. Sathish Kumar, Sateesh Nagavarapu, Arvind K Sharma, "Evaluation of Processing Time and Dataset Size with

using Data Mining Application in Cloude"International Journal of Advanced Research in Computer Engineering & Technology 2278 – 1323

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