iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.31181

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Impact of Data Privacy on Storage in Cloud Computing Ecosystem: A Brief Survey

Megha Singh[1], Dr. Sunita Gond[2]
[1]*Dr APJ Abdul Kalam University*

Abstract: ***Cloud computing has emerged as a boon for numerous fields which are requiring large data storage. It provides a large storage and processing capabilities to consumers through cloud software and services. However, integrity is the serious concern in the loosely interfaced cloud environment. Therefore, assurance of data integrity is the major challenge of diminishing cloud data exploitation activities. Such types of problems are solved using various encryption and decryption methods with time and overhead solving of computing. For this type of issue, data auditing plays an important role which consists of the PDP and POR techniques. Privacy mining algorithms have been suggested in order to protect data privacy. The algorithm does have additional overhead for adding fake things and cannot cover data size. This paper attempts to investigate the impact of privacy factor on users' trust and also attempts to investigate loopholes in existing solution.***
Keywords: Cloud, Cloud Computing, privacy mining algorithm, encryption, decryption.

I. INTRODUCTION

The advent of internet along with the advance communication technologies over the last decade has changed the complete paradigm of computing. The amount of data which could be communicated through these technologies is immense and requires high end storage and processing hardwares. The availability of these state of the art computing technologies is not practicable for all the users due to the cost associated with it.

Even the larger organizations don't prefer to invest a huge sum of money on these tools. Cloud computing has emerged as a solution to this problem. It provides a platform comprises of large storage capabilities and computing capacity to the users on charge as per usage basis. Cloud computing comprises of Public, Private, Hybrid, and Community as its various models. These models are the cloud delivery frameworks which are globally focused on the use of specific security policies to deliver data protection across the network.

With data storage, cloud computing movement and processing present risks and vulnerabilities for cloud data access also. The main challenge with the area of privacy protection is that any user who accesses files may alter the original content of that file. It may result into potential legal consequences. Whenever, it comes up to security, cloud-computing environment becomes risky and face challenges. Prominent challenge here comes up with privacy and security issue. Research on the protection of data privacy in outsourced databases was highlighted with cloud computing growth. Since the outsourced database can contain confidential information, it should be shielded from opponents like a cloud server. The database will then be secured before it is outsourced to the cloud. This paper presents a thorough review to address the severity of the privacy issue and presents the proposed strategies by several researchers.

II. LITERATURE SURVEY

Krithikashree.L et al. In[1] demonstrate study of data audit in cloud for mobile devices. The approach in existing study involves Homomorphic Cryptography with Provable Data Possession (PDP) and Proof of Retrievability (POR) these are the restricted query technique. Third party auditor scheme states data manipulation solution and experimentally results out effective outcome.

Nan Zhangl et al. In[2] described and analyse lightweight solution to resist from attack. This solution seems not to be perfect because of the insufficient solution of attacks. Other attacks are not considered with solution and improved it to achieve complex security with achieving lightweight. An authenticated and authorized solution is proposed by author using Kerberos algorithm.

Anshukirar et al. In[3] proposed cloud parameters like ubiquitous, on-demand and resource based with variety of services. It serves with several services like infrastructure, data storage, hardware etc. Data security with cloud offers weakness due to physical security control, to ensure favourable security a strong approach is required which is extremely valuable. Information outsourcing is also an issue because of protection and privacy of data with multi-tenant environment. Author proposed multi-factor technique for the authentication of multiple users and also preventing illegal cloud access to any unauthorized user.

Table 2.1 Comparison of security models for cloud environment

Title	Author	Year	Methodology Used
A Service-Oriented Middleware for Cloud of Things and Fog Computing Supporting Smart City Applications	Nader Mohamed, Jameela Al-Jaroodi, Sanja Lazarova-Molnar, Imad Jawhar, and Sara Mahmoud	2017 [4]	The concept of fog computing and Cloud of Things (CoT) has been augmented together at the middleware. The potential of fog computing to present a secure data environment is used in this work and the proposed strategy is deployed for smart city applications. The modified version of Internet of Things (IoT) has been proposed in the security architecture.
A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography	Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M. Shamim Hossain	2017 [5]	A combination of fog computing and cryptography has been proposed in this paper to offer an advanced hybrid security model. Pairing based cryptography is used to authenticate the access of the data. The proposed security model is deployed for the healthcare system where the electronic medical record is kept on the cloud. It provided the authentication and access control feature in the hybrid model. However the computation complexity is traded off.
A framework for Data Security and Storage in Cloud Computing	Akshita Bhandari, Ashutosh Gupta, Debasis Das	2016 [6]	The authors have presented a security model which used Hashed Message Authentication code with Index Building for secure storage and sharing of data. For multiple users, fully homomorphic encryption is applied with encrypting and decrypting data securely.
Secure and privacy-preserving pattern matching n Distributed cloud-based data storage	Vladimiri Oleshchuk	2019 [7]	A pattern matching based security and privacy framework has been proposed in this paper. The methodology used modified data structure which is known as index array to add the security and design fast privacy preserving matching algorithm for string machine. The time complexity is tried to be improved in this paper using fast privacy preserving matching algorithm and hence improve the speed of computation in the mentioned environment.
Privacy-preserving Association Rule Mining Algorithm for Encrypted Data in Cloud Computing	Hyeong-Jin Kim, Jae-Hwan Shin, Young-ho Song, Jae-Woo Chang	2019 [8]	The authors have proposed a privacy preserving association rule mining algorithm for encrypted data in cloud computing. A priori algorithm is used in this work by using the EIgamal cryptosystem for association rule mining, without adding extra fake transactions. Thus, the proposed algorithm was able to guarantee both data privacy and query, while concealing data frequency.

III. SUMMARY OF LITERATURE SURVEY

Data privacy and safety are a primary requirement of high end applications these days. Cloud computing is an emerging technology of current era. It has the potential to maximize the computation and storage capacity without investing or wasting in purchasing software or infrastructure. It provides sharing facility based on services for infrastructure, platform and software by minimizing system cost. Bulk usage and business dimension make it popular and need of today's marketplace. Overwhelming use and third-party environment make it supreme target for attackers. Security is another important concern required to achieve trust and brand image of service providers. Low cost and efficient infrastructure sharing make it popular among big organizations to migrate their services on cloud environment. Remote data storage and third party involvement demands security as primary requirement.

This work observe that major issue exist in cloud is the missing of transparency, privacy, lack of authentication, integrity, service level agreement and location of storage which is continuing with the coming years.

Storage transparency is provided to check where your data is stored and in which server, but location tracing is a breach for security. User data is very important and where that important data is travelling and communicating and where it is stored, who is using it are all privacy concern.

Following major problems has been observed in cloud computing:

1) Lack of security provision during communication of data.
2) Privacy is major requirement and concern for user.
3) An efficient storage technique and better integrity verification is required in new solution.
4) Optimization of security algorithms to increase performance of cloud environment.
5) Involvement of fakeness to create makes original data more safe and secure from security thread.

IV. OBSERVATIONS AND DISCUSSION

Several security algorithms have been examined to achieve data privacy by keeping overhead as low as possible. Data privacy can be achieved through cryptographic algorithms which are used to encrypt plain text into cipher text. These algorithms are commonly known as symmetric cryptographic algorithm or asymmetric cryptographic algorithms. Several works considered RSA, AES, ECC, RC4, RC5, RC6 and similar cryptographic algorithm to replace plain text in form of cipher text. Similarly, different integrity algorithms are proposed such as SHA-1, SHA-2, SHA-3, and MD5. Similar to privacy and originality of content, authorization of user is also important. It not only assure about originality of user access but also help to trace who is authorized to access what using access control policy. In this order a significant work has been contributed but all comes with huge overhead. There are so many situations where proposed privacy algorithms raise unnecessary overhead just to achieve level of security. Overwhelming security not only raises computation and memory overhead but also increases response time and access time of primary request.

Privacy of data should be maintained using four parameters like: authentication, integrity, confidentiality and availability.

1) *Authentication:* Authentication is a technology which checks user's credential in database to check user's authenticity. This paper investigates that multilevel authentication, third party authentication, multi server authentication etc need to integrate with current scenarios to enhance the possibilities of authentication.
2) *Integrity:* Integrity protects originality of data by assuring that may not be modified by any unauthorized person. To achieve integrity relevant data is formed in comparison to original data and then that relevant data is divided into chunks and stored in server. If any other person tries to modify it then he will not get original data. Different Integrity policies such as MD5, SHA-1, Checksum need to apply to improve the policy of integrity.
3) *Confidentiality:* Some information needs to be protected due to its confidentiality. Confidential information if leaked may lead to misuse of information. Therefore, protection of such information is essential. Different security algorithms and combination of algorithms such as RSA, ECC, Diffe Hellman, RC4,RC5 ,RC6 and many more can be applied to keep data safe and secure.
4) *Availability:* Availability defines the resource or service availability whenever required to be present for the user. Service denial is common which the attack is and it does not make services available for user
5) *Access Control:* Access control technique assures who can access what. Role based and attributes based access control policy along with hybrid approaches are proposed to achieve such techniques.

Major motivation behind this work is to provide a low overhead framework to improve strength of security. Here, work also expect to integrate different security dimensions such confidentiality, authentication, integrity, access control principles with proposed framework. Broadly, work expect that communication should be done with low computation overhead of encryption as well as decryption time.

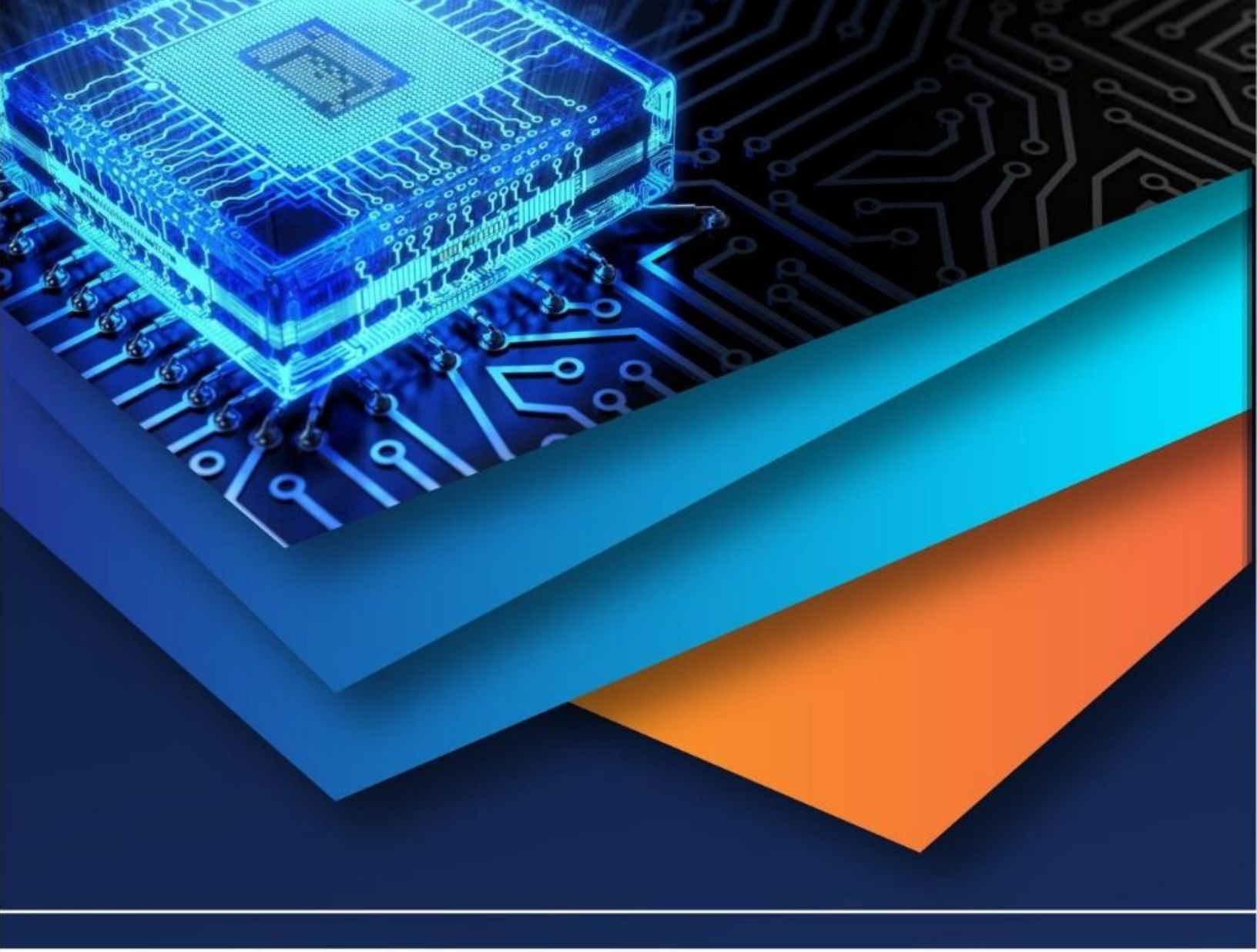
V. CONCLUSION AND FUTURE TRENDS

Outcome expected from proposed research work states that Strong storage and communication model with low security overhead will be achieved. Performance improvement of existing solution and improve level of confusion for attacker. Improved breaching or attacking time is expected as overall outcome of proposed solution. We presented the survey of recently proposed privacy-preserving keyword search scheme specifically to mitigate the privacy issue in cloud data by highlighting the advantages and limitations of the prominent search scheme. This survey demands that a combination of multiple security principles need to integrate as architecture with different algorithms and help to improve the security of cloud computing environment.

The potential of the field of cloud computing and the security issues associated with it has a great scope of research in the future also. The augmentation of some intelligent tools like machine learning algorithms, adaptive security models, and stochastic frameworks may result into a high end security and privacy to the data in the cloud computing environment. The implementation of some state of art encryption and cryptography techniques may also offer some exciting results.

REFERENCES

[1] Krithikashree.L, S. Manisha, Dr.Sujithra.M. Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage. 9th ICCCNT, IISC, Bengaluru India, July 10-12, 2018
[2] Nan Zhangl, Xiaoyu Wul, Cheng Yangl, Yinghua Shenl, Yingye Chengl, "A lightweight authentication and authorization solution based on Kerberos". Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). 3rd, 5th October, 2016 IEEE.
[3] Anshu Kirar, Arun Kumar Yadav and Supriya Maheswari, "An Efficient Architecture and Algorithm to Prevent Data Leakage in Cloud Computing using Multi-tier Security Approach", Proceedings of the SMART -2016, IEEE, 5th International Conference on System Modeling & Advancement in Research Trends , 25th _27'h November, 2016.
[4] Nader Mohamed, Jameela Al-Jaroodi, Sanja Lazarova-Molnar, Imad Jawhar , and Sara Mahmoud, "A Service-Oriented Middleware for Cloud of Things and Fog Computing Supporting Smart City Applications". Smart world, Ubiquitous intelligence & computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big data computing, Internet of people and Smart city innovation, pp. 1-7, 4th_8th August, 2017.
[5] Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M. Shamim Hossain, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography" Vol. 5, 2017, IEEE Access.
[6] Akshita Bhandari, Ashutosh Gupta, Debasis Das, "A framework for Data Security and Storage in Cloud Computing", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).
[7] Yun-Yun Du, Hong-yun Ning, Ping Yang, Yan-xia Cui, "Improvement of Kerberos Protocol Based on Dynamic Password and "One-time Public Key".10th International Conference on Natural Computation, 2014.
[8] Flavio Bonomi, Rodolfo Milito, Jiang Zhu and Sateesh Addepalli, "Fog Computing and its Role in the Internet of Things", In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012.
[9] SK.Md. Mizanur Rahman, Khalil Elkhatib,"Private Key agreement and secure comunication for heterogeneous sensor networks", Journal of Parallel and Distributed Computing 2010, pp. 858 - 870.
[10] Dennis Meffert. Bilinear Pairing in Cryptography. M.S. thesis, Dept. Computer Science, Radboud Univ., The Netherland, 2009.
[11] Alfred Menezes, "An Introduction to Pairing-Based Cryptography", In Recent Trends in Cryptography, American Mathematical Society, 2009, pp. 47-65.
[12] D. Moody, R. Perlner, A. Regenscheid, A. Roginsky and L. Chen. Report on Pairing-based Cryptography. Journal of Research of the National Institute of Standards and Technology 2015, Volume 120, pp. 11-27.
[13] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", In HAWAII International Conference on System Sciences, Koloa, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY