IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENHANCING SECURITY OF CLOUD DATA FROM DATA MINING BASED ON FULLY HOMOMORPHIC ENCRYPTION

Aachal R. Borkar*, Prof. Vijay Bagdi
WCC DEPT. A.G.P.C.O.E, NAGPUR.
WCC DEPT. A.G.P.C.O.E, NAGPUR

DOI: 10.5281/zenodo.50482

ABSTRACT

The advancement in technology, industry, e-commerce and research. A large amount of complex and pervasive digital data is being generated which is increasing at an exponential rate and often termed as Big data. For analyze and handling such big data various tools are available .The cloud computing is resolved for the problems arises in big data storage. Data security is major issues in the cloud can be enhance by fully homomorphic encryption technique. As the cloud, data storage can be manage by clustering for security and privacy of data. In this paper, we have defined of fully homomorphic encryption technique and digital signature is applied to our system and according to that, it shown the output which provide the security to our system.

KEYWORD:. Data security, unauthorized person, Cloud Computing, Security, k-means clustering (4 hosts), Digital Signature.

INTRODUCTION

Cloud computing refers to the web-based computing, providing users or devices with shared pool of resources, information or software on demand and pay per-use basis. It frees a user from the concerns about the expertise in the technological infrastructure of the service. It allows end user and small companies to make use of various computational resources like storage, software and processing capabilities provided by other companies.

Internet has been a driving force towards the various technologies that have been developed since its inception. Arguably, one of the most discussed among all of them is Cloud Computing. The advantages of using cloud computing include: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and highly automated processes wherein the customer need not worry about mundane concerns like software up-gradation.

What is Cloud Computing?

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance.figure1 shows the cloud general model in which the basic purpose model of cloud are used in the structure for the data storage and how the users are accessing the data from the cloud there are number of users of cloud based on the requirement we can established the model for the users as per the requirement of users.

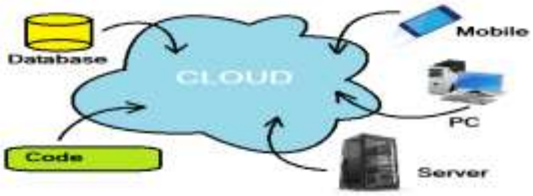

Figure 1. Cloud Model

What is Cloud Taxonomy and Characteristics and Benefits?

According to the different types of services offered, cloud computing can be considered to consist of three layers. Infrastructure as a Service (*IaaS)* is the lowest layer that provides basic infrastructure support service. Platform as a Service (*PaaS)* layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. Software as a Service *(SaaS)* is the topmost layer which features a complete application offered as service on demand.

A. Software as a Service (SaaS)

SaaS ensures that complete applications are hosted on the internet and users use them. The payment is made on a paper- use model. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock". Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). cloud environment is lost. Hence securing the MCS is of great importance.

Mobiles
App Server
SaaS
Networks
Database
Codes
PCs

Figure 2. SAAS

B. Platform as a Service approach (PaaS)

In the *Platform as a Service approach (PaaS)*, the offering also includes a software execution environment.. In case of congestion, there is the problem of outage from a cloud environment.. The data needs to be encrypted when hosted on a platform for security reasons. Cloud computing architectures making use of multiple cryptographic techniques towards providing cryptographic cloud storage.

Figure 3. PAAS

C. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS*)* refers to the sharing of hardware resources for executing services, typically using virtualization technology. Potentially, with IaaS approach, multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged on a pay-per-use basis.

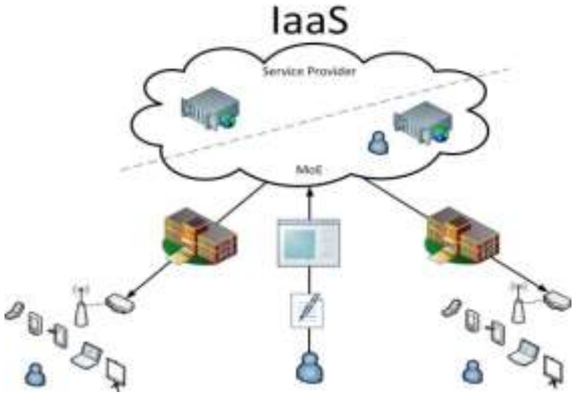

Figure 4. IAAS

LITERATURE SURVEY

Damandeep Kaur, [2], **“**Secure Data Mining in Cloud, Security and privacy “is the major issue concerning the clients as well as the providers of cloud services as a lot of confidential and sensitive data is stored in cloud which can provide valuable information to an attacker. This paper proposes a method to solve the privacy issues of the cloud.Chunhua Su [7], “Privacy-Preserving Two-Party *K*-Means Clusteri viaSecureApproximation”, In this paper, we have proposed a new scheme based secure approximation for privacy-preserving *k*-means clustering. We have solved the security problems in existing scheme and we showed that the output of our scheme is an approximation based on two parties’ joint database. Ranjita Mishra [13], “A Privacy Preserving Repository for Securing Data across the Cloud”, In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase.

FULLY HOMOMORPHIC ARCHITECTURE

In the Gentry’s fully homomorphic scheme, in this technique, the encryption and decryption is based on super key and public key .As compare to other techniques. It contain the faster encryption and decryption at transmitting and receiving. It provides the secure authentication.

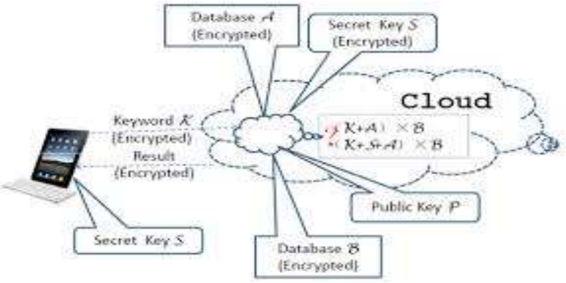

Figure 5. Architecture

SYSTEM DESIGN

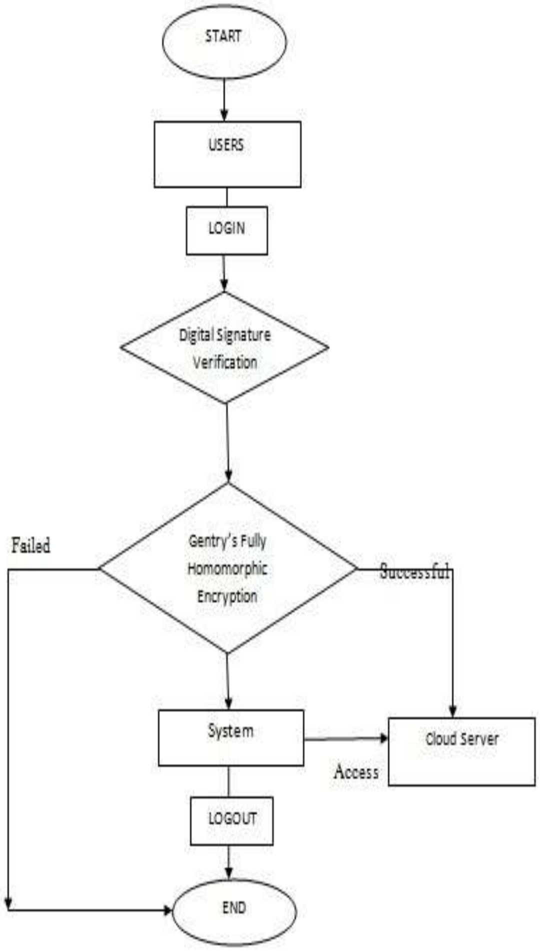
START
USERS
LOGIN
Digital Signature Verification
Failed
Gentry's Fully Homomorphic Encryption
Successful
System
Cloud Server
Access
LOGOUT
END

Figure 6. Data Flow of Project Work

MODULES

In the our proposed system when any user try to use the system it is necessary for that user to register with the details for all need able information is required with the photograph with clear vision and attach digital signature after this all information is saved in the server where authentication is provided and after confirmation it providing information public key is provided to the user and secret key is generated to that user in the server for the particular user by using the fully Homomorphic Encryption.

MODULE I: (REGISTRATION PROCESS)

In our system module one is taken as for the registration process for the all clients as the part of our system is to be using. In that module we have used the Digital signature for the security purposes because it can provide the various levels to add on the single system as the part of security. So following are the different forms for the three levels registration process whenever user has to completed the registration process then he/she can be access to the system.

Personal: In this form user all information is to be filled necessary for using the system as Name , Address, City, Mob no, Email_id is required Email_id is the mandatory for this and it is valid to use our system and in this we have provide the three password for the user as wish to use for the login purpose.

Identification for User: In this second system user need his scan photo and signature. Without photo and signature user can not completed his registration. At the time of login user account he needs his photo and sign which was uploaded at the time of registration. If the photo and sign cannot match, Login will be failed. It is the most important part of this system.

MODULE II: (LOGIN PROCESS)

In the second module of this system contains the login procedure for the user to use the system. User finished its registration then he need to upload his photo and signature again. User should have to upload his photo and sign which he was uploaded at the time of registration. During the process of login he needs to fill his generated Username and password. After this process second option is of uploaded photo. If the photo is match user enter into the User Panel otherwise He will get message that you cannot login account.

MODULE III: (CLIENT SYSTEM UTILITIES)

Once the trusted user is login the system utilities has to be available for the user as Upload, Download, Sending mail and receiving mail and also the number of clients which are working in the particular organization is shown in the system and user can communicate directly with them by simply selecting user then

Upload: In this menu user having the facility to send the attachment to the number of user or client is available without packet loss and communicates directly with the user. And This uploaded file is occur in the encrypted form on the cloud. And because of this high security is occur during the uploading the file. The best Advantages of this encrypted form is no one can directly see the file. The file will be fully secure.

Download: In this menu user having the facility for downloading authenticated files for that user is shown and But user can not download directly this file. He get this file in the encrypted form. To converting file in decrypted form he need to verify his photo and sign. If the photo and sign is match then he can download the file and can be see. but without verification he failed to see.

Sending and receiving Mail: In this menu user having the facility of sending mail to another user but this mail occur in fully secure form. First user gives password to mail. And at the side of receiving User Can see the mail before that he should have to enter his password and verify again photo and signature. After that he will receive mail. Because of his if your account is open at that time no one can see your personal mail.

MODULE IV: (FOUR CLUSTERS)

In this module it contains the four numbers of servers in that the data of users and cloud is saved. If any user wants to access the data the data must be the users of the system also must verify its identity before uploading or downloading the data from the cloud. Data is clustered into four servers in distributed manner so it provides more security as compared to the existing system. And every users wants to access the data to be digital signature is most important otherwise the data will be in the encrypted manner to decrypt it have to verification is necessary.

RESULT ANALYSIS

Table 1
Comparision With Existing system

Sr. No.	Name of contents	Proposed System	Existing System
1	Security Level	2	1
2	Number of Clusters	4	2
3	User Intract at a Time	More	less
4	Packet Loss Rate	2%	4%
5	Memory Overhead	Yes	No
6	Complex	Yes	Yes

7	**Packet Transfer Rate**	**85%**	**75%**
7	**Digital Signature**	**Used**	**No**

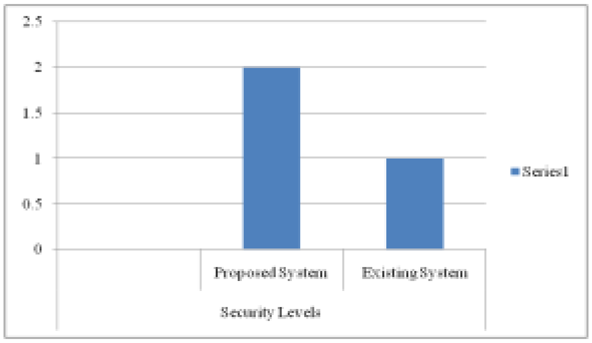

Figure 6. Security Levels

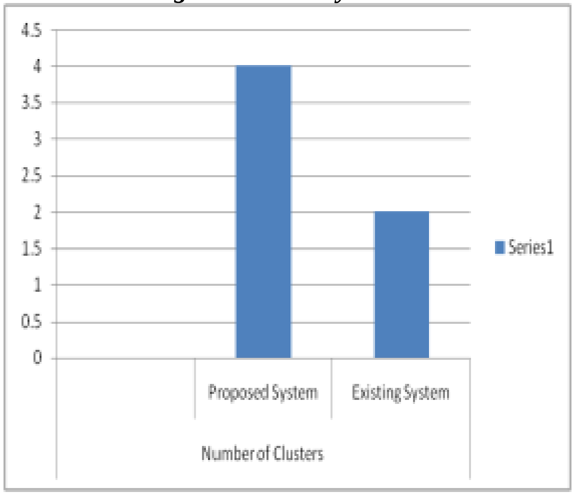

Figure 7. Number of Clusters

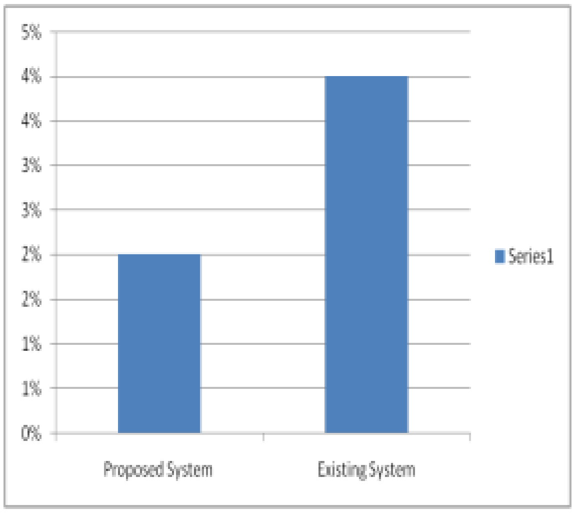

Figure 8. Packet Loss Rate

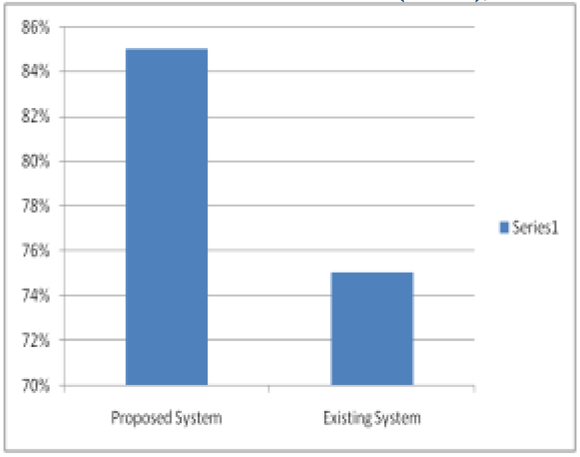

Figure 9. Data Packet Transfer Rate

CONCLUSION

In this paper we briefly describe the Fully Homomorphic Encryption Technique is can be apply on the cloud system for better security and it is providing more security as the techniques applied before as well as clustering is also we can add for better managing the security level for the big data cloud data analysis. We have also implement digital signature on this technique for the better security level of the system.

REFERENCES

[1] Mittal “ Secure Data Mining in Cloud Using Homomorphic Encryption”,Cloud Computing in Emerging Markets(CCEM),2014 IEEE 10.1109/CCEM.2014 7015496.

[2] Su, F. Bao, J. Zhou, T. Takagi, and K. Sakurai, "Privacy-preserving two-party k-means clustering via secure approximation." In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 1, pp. 385-391.

[3] R.Mishra, S. K. Dash, D. P. Mishra, and A. Tripathy, "A privacy preserving repository for securing data across the cloud." In Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol. 5, pp. 6-10. IEEE, 2011.

[4] Q. Lu, Y. Xiong, X. Gong, and W. Huang. "Secure collaborative outsourced data mining with multi-owner in cloud computing." 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom), IEEE, 100-108, 2012.

[5] Veena Khandelwal “Secure and Efficient Data Storage in Multi-clouds”, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 9 (2013), pp. 977-984

[6] Siani Pearson , “Taking Account of Privacy when Designing Cloud Computing Services”

[7] M. Brantner, D. Florescu, D. Graf, D. Kossmann, and T. Kraska, "Building a database on S3." In Proceedings of the 2008 ACM SIGMOD international conference on Management of data, pp. 251-264. ACM, 2008

[8] J. Carolan , S. Gaede, J. Baty, G. Brunette, and J. Weise, "Introduction to cloud computing architecture." White Paper, 1st edn. Sun Micro Systems Inc (2009).

[9] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing." Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS 28 (2009): 13.

[10] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control." In Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85-90. ACM, 2009.

[11] D. J. Solove, "I've got nothing to hide and other misunderstandings of privacy," San Diego L. Rev. 44 (2007): 745.

[12] P. K. Rexer, “Data miner survey highlights the views of 735 dataminers” 2010.IEEE, 2007.

[13] Md. Riyazuddin , Dr.V.V.S.S.S.Balaram ,Md.JaffarSadiq , M.D.Zuber. "An Empirical Study on Privacy Preserving Data Mining". International Journal of Engineering Trends and Technology (IJETT).V3(6):687-693 Nov-Dec 2012. ISSN:2231-5381

[14] K. Che, and L. Liu, "A random rotation perturbation approach to privacy preserving data classification." (2005).

[15] A. Inan, M. Kantarcioglu "Using anonymized data for classification." In Data Engineering, 2009.ICDE'09.IEEE 25th International Conference on, pp. 429-440. IEEE, 2009.

[16] M. V. Dijk, and A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing." IACR Cryptology ePrint Archive 2010 (2010): 305.

[17] H. Dev, T. Sen, M. Basak, and M. E. Ali, "An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks." In High Performance Computing, Networking, Storage and Analysis (SCC), 2012 SC Companion:, pp. 1106-1115. IEEE, 2012.

[18] M. D. Singh, P. R. Krishna, and A. Saxena, "A cryptography based privacy preserving solution to mine cloud data." In Proceedings of the Third Annual ACM Bangalore Conference, pp. 14. ACM, 2010.

[19] S. Pearson, "Taking account of privacy when designing cloud computing services." In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52. IEEE Computer Society, 2009.

[20] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes." In Advances in cryptology—EUROCRYPT’99, pp. 223-238. Springer Berlin Heidelberg, 1999.

[21] K. P. Lin, and M. S. Chen, "Privacy-preserving outsourcing support vector machines with random transformation." In Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 363-372. ACM, 2010.

[22] R. Bhadauria, and S. Sanyal. "Survey on security issues in cloud computing and associated mitigation techniques." arXiv preprint arXiv:1204.0764, 2012.

[23] R. Bhadauria, R. Borgohain, A. Biswas and S. Sanyal. "Secure Authentication of Cloud Data Mining API " arXiv preprint arXiv:1204.0764, 2012.

[24] K. Beaty, A. Kundu, V. Naik, and A. Acharya. "Network-level Access Control Management for the Cloud." 2013 IEEE International Conference on Cloud Engineering (IC2E), IEEE, pp. 98-107, 2013.

[25] I. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis. "Cryptography goes to the cloud." Data Management, and Applications in Secure and Trust Computing, Springer Berlin Heidelberg, pp. 190-197, 2011.