Digital Signature to Secure Data in Cloud Using Homomorphic Encryption-A Review

[1]Tulsi Y Snehi, [2]Prof. Ajaykumar T Shah
[1]Research Scholar, [2]Assistant Professor
Alpha College of Engineering and Technology,
Khatraj, Gujarat, India,

***Abstract*—Cloud Computing has been the most promising innovation in the computing world in past decade. With the advancement in technology, industry 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. Traditional Data Storage systems are not able to handle Big Data and also analyzing the Big Data becomes a challenge and thus it cannot be handled by traditional analytic tools. Cloud Computing can resolve the problem of handling, storage and analyzing the Big Data as it distributes the big data within the cloudlets. In spite of its numerous advantages in both technical and business aspects, cloud computing still poses new challenges particularly in security of Big Data storage. Data Privacy is one of the major issues while storing the Big Data in a Cloud environment. Data Mining based attacks, a major threat to the data, allows an adversary or an unauthorized user to infer valuable and sensitive information by analyzing the results generated from computation performed on the raw data. In this thesis digital signature and homomorphic encryption algorithm are used to protect confidentiality of data stored in cloud by using a secure k-means data mining approach assuming that the data to be distributed among different hosts maintaining the privacy of the data. The approach is able to maintain the correctness and validity of the existing k-means to generate the final results even in the distributed environment.**

***Index Terms*—Cloud computing, data mining, homomorphic encryption, Security, Digital Signature**

I. INTRODUCTION

Cloud computing is the apt technology for the decade. 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 allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. 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. The cloud services can be divided into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[1]. Despite all the above powerful functionalities provided by the cloud computing techniques, a lot of perspective customers and users lack interest for cloud services. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality and authentication is encountered. The users on cloud who uses the service are not always the trusted person so privacy preservation of the data-owner's data is required or it may be possible that any adversary brake the security and hake the original data. Any attacker or adversary having an unauthorized access to the storage on cloud can mine the data and retrieve large amount of confidential data. So security in the cloud is nothing but hide the original data from the service-provider or the user who may be an adversary. Thus security in the cloud is current research topic and in this work research is done to provide the privacy to the data-owner's data from the any attacker or user. Various data analysis techniques or algorithm are available today which can be used successfully to mine valuable information from the large datasets by analyzing the behavioral and statistical data.

II. BACKGROUND THEORIES AND RELATED WORK

Preserving the privacy of the data mining algorithm has been a concern of researchers for long and a number of algorithms have been proposed for the same. Focuses on improving the security of two-party k-means while maintaining the correctness of algorithm. K-anonymity [10], noise transformation and multiplicative transformation are some PPDM (privacy preserving data mining) methods. Compared to PPDM secure cloud mining is a relatively newer field. The attacks in a Cloud Data Mining system can be listed as Denial of Service attack, Distributed Denial of Service, *Sniffing*, *DNS attack*, *Man in the Middle attack* etc. [22] gives a detailed survey on the security issues in cloud and a description of the types of attacks possible in a Cloud Data mining environments with their impact and possible solution to some of them. According to [23] data mining attacks in cloud falls in three classes: network-level, application level and virtualization level. The Network level attacks of the Cloud system and propose a solution for these type of attacks which is deployed on IBM SCE in the form of "Security-as-Service". This application prevents the high-level security attacks. Application level security is discussed in [24]. This discusses various issues regarding the deployment, moving a service on cloud in detail. It mainly focuses on building transparent cloud application using loosely coupled services. Virtualization is the key concept of cloud computing these days but it too act as a loophole in the security of the Cloud. The security of the virtual network residing in a virtual environment. They first discuss the security issues in the virtual machines and network and then propose a solution in the form of a framework to control these security issues but cryptography alone cannot prevent the attacks on the cloud mining systems and some other form of security must also be imposed. Fragmentation technique or partitioning of the database into chunks is another method for security which suggests that keeping the data with different cloud service provider or nodes will prevent an adversary from having the access to complete data and thus will not be able to infer correct results. [25] Discusses the k-anonymity and k-anonymity noise taxonomy in a multi-cloud environment to perform frequent pattern mining. It proves that distributed data or a multi-cloud environment prevents the attacker from getting hold of the complete data thus cannot infer valuable information from the data. A one-time pass key mechanism can be used to preserve the privacy of the user as well as the service provider. This approach is based on the terminology of the authentication of both user and the provider. This paper proposes practical scheme as most of the schemes assumes the models to be semi-honest adversary model. It presents a case study of knn (k-nearest neighbor), SVM (Support Vector Machine) and k-means in the above mentioned outsourced collaborative environment. A lot of Privacy Preserving Data Mining techniques exist today. It finally concludes that most of the existing techniques are an approximation and need to be perfected further if efficiency and accuracy is required as most of the algorithms compromise one for the other and to get a balance between them more robust, dedicated and perfect PPDMs are required. Along with this PPDMs authentication between cloudlets is also required..

III. LITERATURE REVIEW

Many researchers have attempted to provide security in cloud using different encryption techniques. Here is the observation summarization of each & every research done.

Ms. Deepti Mittal along with his team has stated an encryption technique called Secure data mining in cloud using homomorphic encryption technique. The proposed approach performs k-means clustering of a dataset which is partitioned horizontally and stored two distinct areas. The methodology first run locally then performs a combined calculation on encrypted results to get complete result. The assumed model is semi-honest adversary i.e. members attempt to release the information of each other while keeping up their security. But this study was performed only on limited nodes and it does not provide third party security during communication.. This system works well but can be made more reliable if authenticity will get provided.

Mr. Shashank Bajpai and his team have introduced the more reliable solution to secure data in cloud using fully homomorphic encryption technique. This paper proposes security ensurement both in Public Cloud and Private Cloud. The proposed system is used to send data to the cloud providers. Thus enabling of cloud computing vendor is done to perform operations on data as per request, such as analyzing sales patterns, without exposing the original data. This can be achieved by cryptosystems based on Homomorphic Encryption. Authors recommend to improve homomorphic encryption algorithm's complexity and response time to requests gets calculated according to the length of the public key.

Mr. Aws Naser Jaber and his team does study in data security in cloud. They studied on real Service suppliers, for example, Microsoft, Yahoo, and Google, have subsequent to added encryption to end-to-end information facilitating and administration for clients. For instance, Google Cloud Storage now consequently scrambles every single new data written on disk. As indicated by specialists, measures are critical for securing the development of knowledge between the customer organizations and the suppliers of cloud services. Ordered archives from the NSA demonstrate that they are attempting to debilitate encryption calculations utilized by people in general. As indicated by the US government, Cloud administration firms must hand over their encryption keys when inquired. Such articulations have centered significant consideration on key administration and information proprietorship. A cloud framework administration organization, affirmed that in spite of the fact that encryption endeavors by administration suppliers have fundamental influence in enhancing cloud security, their adequacy is constrained.

Mrs. Uma Somani and her team have implemented Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing. In this research they have studied data security in cloud using RSA algorithm. Cloud computing is the Concept Implemented to unravel the Daily Computing Problems, preferences of Hardware Software and Resource Availability unhurried by Computer clients. The distributed computing gives an undemanding and non-incapable Solution for Daily Computing. The common Problem Associated with Cloud Computing is the Cloud security and the proper Implementation of Cloud over the Network.

Mr. Khalid El Makkaoui and his team has studied Challenges of Using Homomorphic Encryption to Secure Cloud Computing. In this paper challenges of using homomorphic encryption techniques are discussed. Cloud computing providers must implement concepts ensuring network security, hardware, data storage and strategies of control and access to services. All these elements help to preserve data security and ensuring the availability of services associated with the Cloud, to better satisfy clients and acquire and build their trust. Even if the data storage security in cloud servers is assured, reluctance remains when it comes to process the confidential data. The fear that sensitive data is being used is a major obstacle in the adoption of cloud services by enterprises. Authors recommended focusing on the analysis and improvement of the complexity of existing Homomorphic Encryption algorithms by enabling cloud servers for performing various operations by the clients and providing assurance of the quality of service.

So, in general there is scope of improvement in accuracy, privacy, security and authenticity in cloud computing environment and still there is a scope of research in the area to improve the security during the mining of data using cloud computing techniques.

IV. RESEARCH GAP & CONCLUSION

After observing many research methodologies in cloud it seems that there are many systems which have been implemented with different encryption techniques and authentication techniques. But still there is a scope of improvement by providing authenticity between users and higher security during transmission of data between client and requester of data. By improving these factors a more accurate and secure transaction of data will get achieved in cloud environment.

V. Acknowledgement

It is a matter of great pleasure for me to get this opportunity of expressing my deep and sincere gratitude to those who has always helped me throughout my work. I heartily thank my guides Mr. Ajaykumar T Shah for providing me their valuable guidance and constant support in my work. They guide me with their excellent knowledge in the area of "Digital Signature and Encryption Algorithms". I would also like to thank all my colleagues who have helped me in some way or the other. I would like to thank my parents & family member for their love and support to build my moral during the work.

References

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

[2] 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.

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

[4] Shobha Rajak, Ashok Verma "Secure Data Storage in the Cloud using Digital Signature Mechanism" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.

[5] T. Sivasakthi and Dr. N Prabakaran" Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014.

[6] Wojciech Kinastowski" Digital Signature as a Cloud-based Service"The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, CLOUD COMPUTING 2013.

[7] Deepti Mittal, Damandeep Kaur, Ashish Aggarwal" Secure Data Mining in Cloud using Homomorphic Encryption " Cloud Computing in Emerging Markets (CCEM), 2014 IEEE International Conference.

[8] ZhenQiWang; HaiLongLi"Research of Massive Web Log Data Mining Based on Cloud Computing"Computa tional and Information Sciences (ICCIS), 2013 Fifth International Conference.

[9] Devadkar, K.K." Secure cloud mining"Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference.

[10] Jian Li; SicongChen; DanjieSong"Security structure of cloud storage based on homomorphic encryption scheme"Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference.

[11] Shashank Bajpai and Padmija Srivastava" A Fully Homomorphic Encryption Implementation on Cloud Computing" International Journal of Information & Computation Technology 2014.

[12] Jaber, A.N.; Bin Zolkipli, M.F.; Binti Abdul Majid, M.; Khan, N.U." A study in data security in cloud computing "Computer, Communications, and Control Technology (I4CT), 2014 International Conference.

[13] Vagdevi,S."A mixed homomorphic encryption scheme for secure data storage in cloud"Advan ce Computing Conference (IACC), 2015 IEEE International

[14] Pawar,Y."Use of Digital Signature with Diffie Hellman Key Exchange and AESEncryption Alg orithm to Enhance Data Security in Cloud Computing "Communication Systems and Network Technologies (CSNT), 2013 International Conference

[15] Ezzati,A.; Hssane,A.B."Challenges of using homomorphic encryption to secure cloud compu ting"Cloud Technologies and Applications (CloudTech), 2015 International Conference

[16] Lakhani,K.; Mundra,M."Implementing digital signature with RSA encryption algorithm to enhan cethe Data Security of cloud in Cloud Computing"Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference [17]Sandha; Durga,M.G."Study on data security mechanism in cloud computing"Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference

[17]Gupta,C.P.; Sharma,I."A fully homomorphic encryption scheme with symmetric keys withapplication to private da ta processing in clouds"Network of the Future (NOF), 2013 Fourth International Conference

[18]Chunhua Su; Feng Bao; Jianying Zhou; Takagi, T.; Sakurai, K." Privacy-Preserving Two-Party K- Means Clustering via SecureApproximation"Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference

[19]S. Owen, A. Robin, T. Dunning, and E. Friedman. Mahout in Action. Manning Publications, 2012.

[20]C. Tai, J. Huang, and M. Chung. "Privacy Preserving Frequent Pattern Mining on Multi-cloud Environment." 2013 International Symposium on Biometrics and Security Technologies (ISBAST), IEEE, pp. 235-240, 2013

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

[22]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

[23] http://storage.googleapis.com/books/ngrams/books/datasetsv2.html