IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SECURITY OF CLOUD DATA IN 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.

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 analyse and handling such big data various tools are available.The cloud computing is resolved for the problems arrises 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, a brief introduction of fully homomorphic encryption technique and digital signature can be also applicable as security in future aspect.

KEYWORDS: 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. Over the last few years, cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its users and providers. 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.

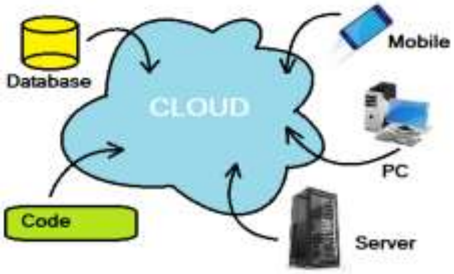


Figure1. Cloud Model

WHAT IS CLOUD TAXONOMY AND CHARACTERISTICS AND BENEFITS?

Cloud computing can be classified based on the services offered and deployment models. 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 payper- use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. 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). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.

Mobiles
App Server
SaaS
CRM
Marketing
Networks
Database
Codes
PCs

Figure2. SAAS

B. Platform as a Service approach (PaaS)

In the *Platform as a Service approach (PaaS)*, the offering also includes a software execution environment. For example, there could be a PaaS application server that enables the lone developer to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. 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.

Figure3. 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 [10]. They are all virtual machines, which need to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information.Data mining can be a serious threat to the cloud security. Specially, to the organizations dealing with the financial, governmental, education or legal issues of people, leaking of which can sometime result in national catastrophes for e.g. collection of financial, health etc information by TIA (Total Information Awareness) in 2002 [5] and analysis of phone records of people gathered from phone companies by NSA for identifying the possible terrorists in May 2006[5]. Also, according to a survey conducted by Rexer analytics, 7% of the data miners analyze the data using the cloud [6], due to the cheap and elastic computing powers offered by the cloud computing. So, maintenance of client privacy goes in parallel with data privacy in cloud and is a major area of concern for the cloud provider as well as cloud user.

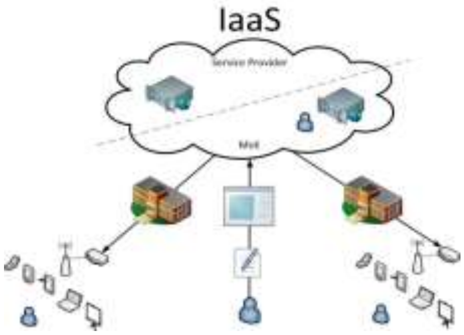


Figure4. IAAS

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. It assumes that the user data is distributed on two hosts and performs a combined k-means clustering using the Pallier Homomorphic encryption system for security purpose so as to prevent any interpretation of intermediate results by an attacker. The proposed approach can further be extended by adding a digital signature or hashing technique to authenticate the third party so as to prevent an adversary from posing as the third party to host's. Also it can be generalized or extended to more number of hosts if required.

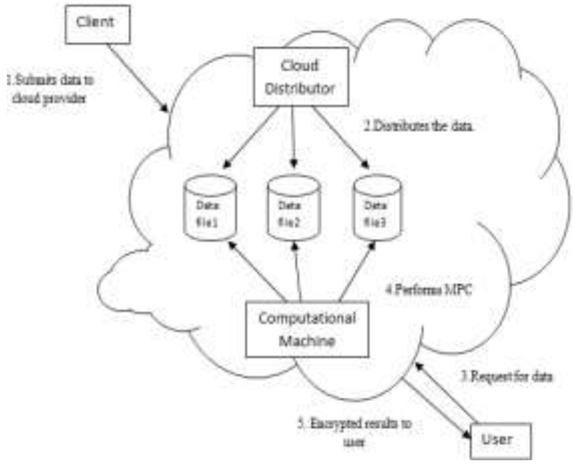


Figure5. Overview of the Proposed Approach

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. It can overcome the correctness problem in scheme based on oblivious polynomial evaluation. And we have showed that our scheme is more efficient with low communication and computation complexity compared to the existing schemes. Existing privacy-preserving *k*-means scheme including ours all deal with the semi-honest model. It is a challenging future work to solve the privacy-preserving problem under an active adversary model in which the participants of the protocol substitute their local input. And we also will use cryptographic techniques in other data mining methodologies such as association rule mining, EM classification and link analysis for large databases.

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. In our paper we are laying stress on the security issue in the cloud. The proposed scheme is probably secure under the standard security model [22]. In addition, our proposed scheme is able to support user accountability with minor extension. Whether you are assembling, managing or developing on a cloud computing platform, you need a cloud-compatible database. The shared-disk database architecture [23], on the other hand, does support elastic scalability. It also supports other cloud objectives such as lower costs for hardware, maintenance, tuning and support. It delivers high-availability in support of Service Level Agreements (SLAs). As with every tectonic shift in technology, there is a Darwinian ripple effect as we realize which technologies support these changes and which are relegated to legacy systems. Because of their compatibility, cloud computing will usher in an ascendance of the shared-disk database. The privacy preserving repository delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

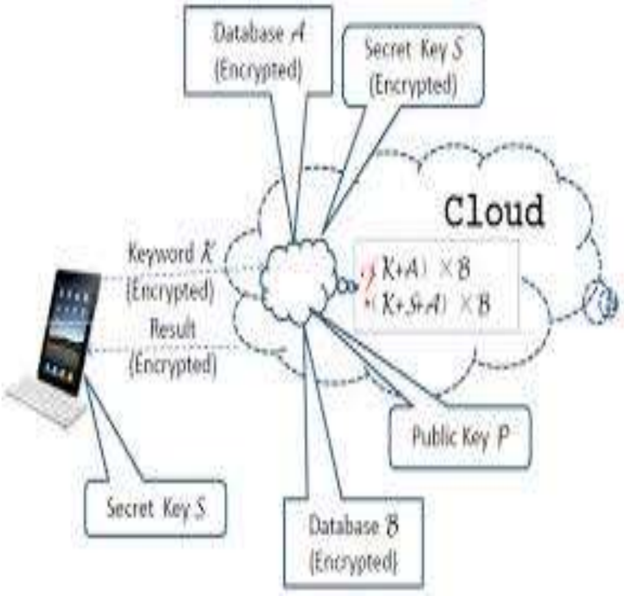
Qiwei Lu, [25], Secure Collaborative Outsourced Data Mining with Multi-owner in Cloud Computing, In this paper, we explore the collaborative outsourced mining condition with multi-owner in cloud computing model. As a case of study, three classical methods KNN, K-means and SVM are analyzed respectively. We design the overall framework for it and propose several enhanced scheme under different security assumptions and conditions. The final framework will utilize trusted computing technology to detect the malicious cloud. At last, we do the security and efficiency analysis for the frameworks and schemes proposed in this paper. In the future, our study and work will focus on following aspects: 1) the further formal security analysis and proof of the schemes proposed above; 2) the measurement of the trusted cloud configuration should be further studied and refined; 3) the extension of the frameworks and schemes.

Veena Khandelwal [7], "Secure and Efficient Data Storage in Multi-clouds", In this paper we have used categorization, fragmentation, distribution and replication techniques to ensure secure and efficient storage in clouds. Data fragmentation uses privacy constraints fragmentation along with horizontal and vertical fragmentation so that any information if in any case becomes available to either the Cloud Database as a Service Provider or to any outsider is of no value. So the data stored is secured. Also the data chunks are replicated at more than one service providers so as to ensure availability, allow concurrent access, restricts data mining attacks and reduce data transfer cost.

Siani Pearson [8], Taking Account of Privacy when Designing Cloud Computing Services, We have argued that it is very important to take privacy into account when designing cloud services, if these involve the collection, processing or sharing of personal data. Privacy should be built into every stage of the product development process: it is not adequate to try to bolt on privacy at a late stage in the design process. Furthermore, we have suggested a variety of guidelines and techniques that may be used by software engineers in order to achieve this, in particular to ensure that the risks to privacy are mitigated and that data is not excessive, inaccurate or out of date, or used in unacceptable or unexpected ways beyond the control of data subjects.

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.



CONCLUSION

In this paper we review 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 can also implement digital signature on this technique for the better security level of the system.

REFERENCES

[1] 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.

[2] 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).*

[3] 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.*

[4] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, 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.*

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

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

[7] C. 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.*
IEEE, 2007.

[8] Md. Riyazuddin , Dr.V.V.S.S.S.Balaram , Md.Afroze , 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*

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

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

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

[12] 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.*

[13] 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.*

[14] 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.*

[15] 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.*