Review on Data Security on Cloud using Homomorphic Encryption over Big Data

Rinkal Patel[1]

[1]PG Student, B.V.M. Engineering College, V.V. Nagar, Gujarat, India.

---***---

Abstract—: *Over a period of the last decade, cloud computing has been the most emerging technology with steady growth. Traditional data storage systems are not able to handle large amount of data and analysis of those data. That's where cloud computing comes into the picture as it has massive amount of storage and management capability where vast information can be deposited inside the cloudlets. By using data mining attacks, one can easily gain unauthorized access to valuable and sensitive information of Big Data, the consequences of which can be fatal. My aim is to protect confidentiality of data stored in cloud by making the use of digital signature and homomorphic encryption algorithm. Using a secure k-means data mining approach I will divide the Big Data, expecting that the data to be divided among various hosts while keeping the privacy. The methodology can maintain the accuracy and validity of the current k-means to produce the final results even in the distributed environment.*

***Keywords*—Homomorphic Encryption, HDFS, k-means.**

1.INTRODUCTION

Main goal of cloud computing is to share os, applications, storage, data and processing capacity among users. Cloud computing is an emerging computingtechnology that uses the internet and central remote servers to maintain data and application on cloud. Cloud computing collects all the computing resources and manages them automatically through software [5]. The users need not care how to buy servers, software solutions and so on. Users can buy the computing resource through internet according to their own needs. Cloud Computing has emerged as an important paradigm that has attracted considerable attention in both industry and academia[6].five essential characteristics of Cloud Computing namely: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. 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). A cloud might be restricted to a single organization or group (private clouds), available to the general public over the Internet (public clouds), or shared by multiple groups or organizations (hybrid clouds) [5].

Cloud Computing security challenges and it's also an issue to many researchers; first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud[6]. Above issues Security comprising of data privacy issue or confidentiality of data is one of the major [1].Lot of advantages are bring for the use of cloud computing like reduced costs, easy maintenance and re-provisioning of resources. As all the data resides with the cloud provider, a serious data privacy issue arises if the provider misuses the data or the information [1].

This paper perform k-means clustering Algorithm of the data set which is partitioned horizontally using "HDFS" and gathered numbers of nodes. The methodology first run locally and then performs "k-means" for combined data on encrypted result to get complete (final) result. And after then run on "HDFS" and also then perform same above steps.

2.LITERATURE SURVEY

A) Title : Secure Data Mining in Cloud using Homomorphic Encryption [1].

Summary : They are provides secured mining of data in cloud using "homomorphic encryption" encryption technique. Here proposed approach perform k-means clustering Algorithm of a data set, which is partitioned horizontally using "HDFS" and save two nodes. This methodology first run locally and then implement "k-means" for combined data on encrypted result to get complete(final) result.

B) Title :A Fully Homomorphic Encryption implementation on Cloud Computing Encryption[2]

Summary: They are propose security ensurement both in public and also private cloud. The proposed system is used to send data to the cloud providers. Thus enabling of cloud computing merchant is done to perform operations on the data as per user call, such as analyzing sales patterns, beyond exposing the real data. This can be achieved by cryptosystems based on "Homomorphic Encryption". Three type of homomorphic encryptions are possible.1)partial HE, 2) somewhat HE, 3) fully HE. Authors recommend to enhance HE algorithm's complexity and response time to requests gets calculated according to public key length.

C) Title :A Study in Data Security in Cloud Computing [3].

Summary: In this paper they are provide data security in cloud is concluded. Real service provider Company, for example Google, Yahoo, Microsoft 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 providers of cloud services. Ordered archives from the NSA demonstrate that they are attempting to debilitate encryption calculations in general utilized by people.

D) Title : Challenges of Using Homomorphic Encryption to Secure Cloud Computing [4]

Summary: In this the different Homomorphic Encryption systems (Partially, Somewhat and Fully Homomorphic Encryption), the few challenges resulting of using this concept and new Client-Cloud provider Architecture, that can improve the performance of this technique. Writers recommended to mainly focus on the analysis expand of the complexity of existing HE algorithms by enabling cloud server for operating various operations by the clients and provide assurance of the Quality of Service (QoS)

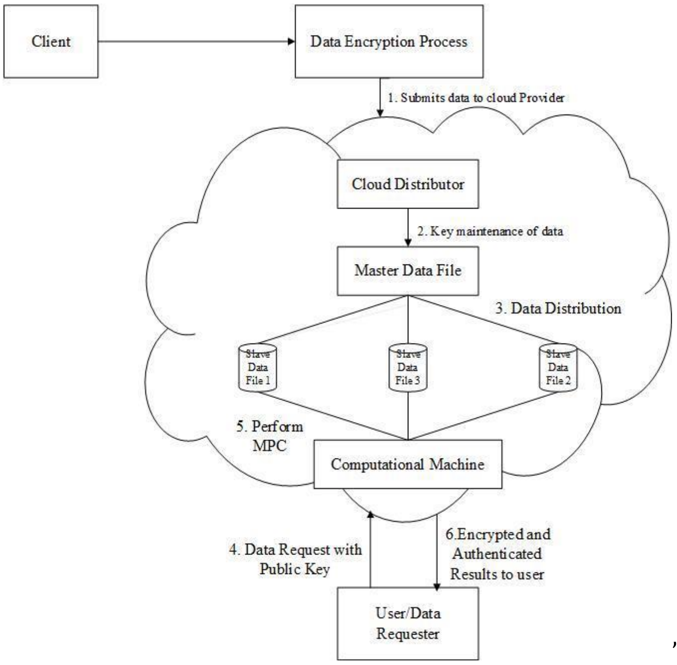
E) Title : Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing [5]

Summary: In this paper the study of data security using RSA algorithm. Cloud computing is the Concept Implemented to unravel the Daily Computing Problems, conduct of Hardware Software and Resource Availability unhurried by Computer consumer. The distributed computing gives an undemanding and non-incapable Solution for cyclic Computing. The normal problem combined with Cloud Computing is the Cloud security and the proper Implementation of Cloud over the Network.

3.RELATED WORK

The Proposed system improves security and data integrity in thecloud environment. It guess that the user's data is not stored in centralized location but is distributed location and performs a combined k-means clustering algorithm. The proposed system is a hybrid of previously studied systems where the security will be provided using mainly two encryption techniques. Digital Signature is used to provide authenticity of a message or process which is a one type of mathematical scheme. If the given digital signature is correct then that will provide detail that the message is created by known sender and the data residing in that is not altered. K-means clustering is used to mine from given data along with that it maintains the privacy of data from both the side to prevent leakage of intermediate result by an attacker. It will provide input and final outputs to the host and user does not have to bother about intermediate results.

Homomorphic Encryption: Homomorphic encryption, it is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its real form [4]. Homomorphic encryptions allow complicated mathematical operations to be performed on encrypted data without compromising the encryption [9].



”

Figure 2: Overview of Proposed System[1]

In mathematics, homomorphic define the transformation of one data set into another data set while preserving relationships between elements in both data sets. The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the equivalent structure, identical mathematical operations whether they are performed on encrypted or decrypted data will yield equivalent results. Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Here is a very plain example of how a homomorphic encryption scheme might work in the cloud computing:

For Example: 1) university ABC has a very important data set and that consists of the numbers 10 and 20. Now to encrypt those data set, university ABC multiplies each element in the set through 4. After successfully finished this operation created new set whose members are 40 and 80. 2) University ABC sends the encrypted very important data set to the cloud for secure data storage. A few months or years later, the government contacts university ABC and requests the sum of very important data set elements. 3) university ABC is too much busy at that time, so it asks the cloud provider to perform the plus operation. The cloud provider, who only has access to the encrypted data set, find the sum of 40 + 80 and then recovery the answer 120. 4) university ABC decrypted that cloud provider's reply (decrypt that result with divide by 4) and provides the government with the decrypted last final answer,30[8].

There are three(3) types of homomorphic encryption: Fully Homomorphic Encryption (FHE) and Somewhat Homomorphic Encryption (SHE) and partial HE[3]. Each type differs in the number of operations that can be performed on encrypted data. FHE allows for an unlimited, arbitrary number of computations (both addition and multiplication, generally minus not possible) to be performed on encrypted data. SHE cryptosystems support a limited number of operations (i.e., any amount of addition, but only one multiplication) and are faster and more compact than FHE cryptosystems [5].

4.CONCLUSION

After surveying many types of research for data security on cloud using homomorphic encryption it appears that "Digital Signature to Secure Data in Cloud Using Homomorphic Encryption", basically provides a system to solve the privacy issue of cloud. In this user data is distributed on two different hosts and key also pass through cloud and then performs a combined k-means clustering using Pallier Homomorphic encryption system to prevent interpretation of intermediate attacker. So there is a wide scope of user data is distributed on more than two different hosts and key not pass through cloud.

REFERENCES

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

[2] Shashank Bajpai andPadmija Srivastava. "A Fully Homomorphic Encryption implementation on Cloud Computing" International Journal of Information & Computation Technology. ISSN 2014.

[3] Aws Naser Jaber1, Mohamad Fadli Bin Zolkipli2. " A Study in Data Security in Cloud Computing" International Conference on Computer, Communication, and Control Technology 2014.

[4] Khalid EL MAKKAOUI, Abdellah EZZATI. "Challenges of Using Homomorphic Encryption to Secure Cloud Computing" 2015 International Conference on Cloud Technologies and Applications (CloudTech).

Uma Somani,Kanika Lakhani,Manish Mundra. " Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC – 2010s).

[5] M. TEBAA and S. EL HAJII. "Secure Cloud Computing through Homomorphic Encryption, " International Journal of Advancements in Computing Technology (IJACT), Vol.5, No.16, pp. 29 –38.

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

[7] http://searchsecurity.techtarget.com/definition/homomorphic-encryption

[8] http://en.wikipedia.org/wiki/Homomorphic_encryption

[9] 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).

[10] 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.