Homomorphic Encryption Scheme to Secure Data Mining in Cloud Computing for Banking System

[1]Ms. Rita Karare, [2]Ms. Dimple Piprewar, [3]Ms.Pritee Bisen
[4]Ms. Vaishnavi J.Deshmukh

[1, 2, 3]B.E Student, Department Of Computer Science and Engineering, Smt.Rajshree Mulak College of Engineering for Women, Nagpur, India
[4]Assistant Professor, Department Of Computer Science and Engineering, Smt. Rajshree Mulak College of Engineering for Women, Nagpur, India
[1]ritakarare12@gmail.com, [2]dimple.piprewar22@gmail.com, [3]bisenpriti123@gmail.com, [4]vjd03redifmail.com

Abstract: *Big data is difficult to handle, process and analyse using traditional approach. Using services, we can resolve problem like resource sharing, storage capacity and data transfer bottlenecks etc. But there is a main issue of data mining based attacks, allows an adversary or an unauthorized user to extract valuable and sensitive information by analysing the results generated from computation performed on the raw data. In order to provide privacy, security for cloud user as well as cloud provider. We proposed a system for secure data mining using well known techniques like homomorphic encryption system, RSA algorithm. In this process flow, cloud server is unware of data uploaded by the user and the client only gets the computational results. Through an experimental evaluation, we can maintain correctness and confidentiality of final result.*

Keywords: *Homomorphism Encryption, Decryption, Data mining, Security*.

1. INTRODUCTION:

Cloud computing is a kind of Internet-based computing that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. 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. To maintenance of client privacy along with data privacy in cloud is a major area of concern for the cloud provider as well as cloud user.

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 in the raw data. 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.

The homomorphic public key encryption is a cryptographic system that allows the performance of a set of operations on the data when they are encoded, resulting in its data appearing in plain text. 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. It can resolve the problem of handling, storage and analyzing the Big Data.

Security is the prime requirement because of the increasing usage of the internet of public cloud for storing the data. Security is needed for preserving the integrity, confidentiality, availability of the information system resources. There can be storage of the data in the encrypted format in any database but if the operations or the computations on the encrypted data are required to be performed then it is the necessary to decrypt those data but the decrypted data are not secure any more thus, a new idea of the cryptosystem was proposed that allows the direct computation on the encrypted data.

2. LITERATURE REVIEW:

Security threat issues and countermeasures in cloud computing: they have stated that this system is mainly focuses on security threats of cloud computing system also they mention some solution and countermeasure on this security problem, it highlighted all these issue of cloud computing. It is totally internet based technology where the resources and information shared on a distributed network, so it is important for both provider as well as consumers to provide the security and trust to shared .the data for developing cloud computing application. Because organization are now moving fast towards the cloud so there is a possibility of threats that will harm the data on the cloud. [1]

Improving Cloud Security Using Data Mining: they have stated that, this system propose and efficient distributed architecture to mitigate the risks. New attacks are being discovered every day and new countermeasure have to be develop to keep data secure. Attackers and providers efficient data mining technique to extract information about the user from the data stored in cloud. With increase in sharing of data over web there is an increase in possibility of data being subjected to malicious attacks .Attackers /provider can extract sensitive information by analysing the client data over a long period of time. Hence the privacy and security of user data is compromised. [2]

Cloud Computing security- Trends and research Directions: they have stated that, it take a holistic view of cloud computing security-spanning across possible issue and vulnerabilities connected with virtualization infrastructure software platform; identity management and access control; data integrity ; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. Cloud computing as a platform for outsourcing and remote processing of application and data is gaining rapid momentum. Security concern; especially those around platform, data and access; can prove to be hurdles for adoption public and hybrid cloud. [3].

Security and Privacy in Cloud Computing: They have stated that, beginning with these attributes, they present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. When outsourcing the data and business application to a third party causes security and privacy issues to become a critical concern. Throughout the study at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issue in cloud environments. [4]

Survey on recent algorithms for privacy preserving data mining: They have stated that, privacy preserving data mining is an emerging technology which performs data mining operations in centralized or distributed data in a secured manner to preserve sensitive data. A number of techniques such as randomization, secured sum algorithm and K-anonymity have been suggested in order to perform privacy-preserving data mining. In this paper, a survey on recent researches made on privacy preserving data mining techniques with fuzzy logic, neural network learning, secured sum and encryption algorithm is presented. [5]

Data Mining Approach in Security Information and Event Management: This paper gives an overview of data mining field& security information event management system. How various data mining techniques can be used in security information and event management system to enhance the capabilities of the system .

Data mining is becoming increasingly common in both the private and public sectors. The real problem in today's enterprise security is amount of logs generated by various systems. Organizations often put too much faith in their new shiny firewalls. The drawbacks of this system use other data mining technique like classification, clustering to enhance the system capacity. Various techniques have been introduced to reduce false positive alerts and reduce CPU loads on system. [6]

3. MATERIALS:

Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is sometimes a desirable feature in modern communication system architectures.

A. Algorithm

RSA (Rivestmk-Shamir-Adleman) Algorithm-

In this system we use RSA (Rivest-Shamir-Adleman) Algorithm, it involves four steps: key generation, key distribution, encryption and decryption. RSA involves a public key and private key. The public key can be known by everyone, and it is used for encrypting messages. RSA is one of the first practical public key cryptosystems and is widely used for secure data transmission.

1. Key Generation-

Step 1: Each user generates a public/private key pair by selecting, two large primes at random- p,q.
Step 2: Computing their system modules N=p.q and (N)=(p-1)(q-1)
Step 3: Selecting at random the encryption key e Where, 1<e< (N), gcd (e (N))=1
Step 4: Publish their public encryption key:
KU={e,N} n keep secret private decryption
Key: KR={d,p,q}

2. Encryption-

Step 1: Obtain public key of recipient KU={e,N}
Step 2: Computes: C=M mod N, WHERE 0<M<N

3. Decryption-

Step 1: Uses their private key KR={d,p,q}
Step 2: Computes: M=C mod N

4. ANALYSIS:

The main goal of the system is to provide the security of the data, to take the backup of the data retrieve of the data. The approach is able to maintain the correctness and validity of the existing k-means generate the final results even in the distributed environment. A new approach of modern cryptography, defined as the Homomorphic Encryption allows for the encrypted data to be arbitrarily computed which is a solution that aims to preserve the security, confidentially and data privacy. This system proposes methods that ensure the confidentiality and privacy in the mining of databases based on fully Homomorphic Encryption. The problem statement proposes a secure data mining approach assuming the data to be distributed among different hosts.

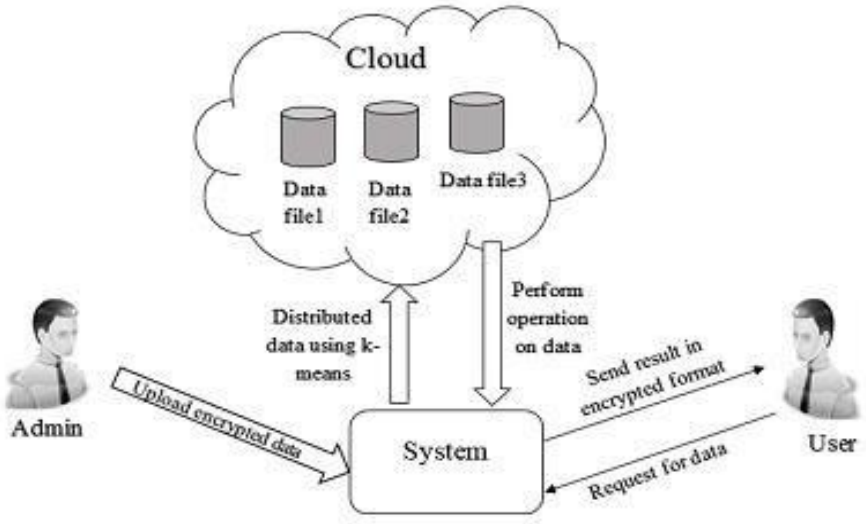

Fig. System Architecture of proposed system.

A. Account Creation-

In this module, first of all user can register their Name, Address, and Mobile Number, Email id, and all personal information for applying new account. System intended for use by the general public often allow any user to register simply by selecting a register or sign up function and providing these credentials for the first time. Registered users may be granted privileges beyond those granted to unregistered users.

B. Checking Credentials-

In this module, if user can fill all the required personal information correctly then admin can approve/disapprove the user request. They include the ability to approve or disapprove user

Request without restriction. When admin approve the request of user the user gets a mail of user name, password and one part of encrypted image.

C. Encryption-

Encryption secures online information, protects from countless daily attacks, in encryption is the process of encoding a message or information in such a way that only authorized parties can access it. In this process User's ID proof is encrypted, and one third part of that encrypted image will be send through the mail by admin.

D. Transaction-

Users online banking system that consist of transfer money, statement, account details and money, amount have to be entered to transfer then user go to the Transaction to transfer then user.

E. One Time Password (OTP) Generation-

After clicking on transfer the user gets an email of OTP security code that is useful for more security by user side. OTP have time limit for 30 seconds, after typing correct OTP code the amount transfer successfully.

E. Decryption-

Decryption is the process of taking encoded or encrypted image or other data and converting it back into image that user can read and understand, that one third part of encrypted image will be decrypted in this process. If both user and admin data will be match then user get a user ID and password.

5. ACKNOWLEDGEMENT:

We would like to extend our heartfelt thanks to our project guide, **Ms. Vaishnavi J. Deshmukh** acknowledge herable guidance and constant encouragement, which went to long way in ensuring our success. Her vast knowledge and experience in the field of computer was of immense help to us during the paper publication. Also I am thankful to my Department for the technical support.

6. CONCLUSION:

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. The proposed system solves 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 Homomorphic encryption system for security purpose so as to prevent any interpretation of intermediate results by an attacker.

Security of cloud computing based on fully homomorphic encryption is a new concept of security which is to enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculations was carried out respecting the confidentiality of data.

REFERENCES:

1. Deepti Mittal, Damandeep Kaur, Ashish Aggarwal, "Security threat issues and countermeasures in cloud computing". IEEE Cloud Security.
2. Sunanda Ravindran, Parsi Kalpana, **"**Improving Cloud Security Using Data Mining", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4.
3. Hemalatha ,Dr. R. Manickachezian, "Cloud Computing security- Trends and research Directions", International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, Issue 11,
4. Mr. V. Biksham, Dr. D. Vasumathi, "Security and Privacy in Cloud Computing", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
5. S. SelvaRatna , Dr. T. Karthikeyan, "Survey on recent algorithms for privacy preserving data mining", S.SelvaRathna et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1835-1840.
6. ShashankBajpai, PadmijaShrivastava, "Data Mining Approach in Security Information and Event Management", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8.
7. V. Bhagat, "Novel Approach towards higher security using crypto-stego technology", International journal of emerging trends and technology in computer science (IJETTCS), Vol.04, issue-1, PP.
8. V.Bhagat," Cross Cloud single sign on (SSO) using token ", International journal of research of engineering of technology (IJRSET), Vol.02, issue 07, PP. 271-247.