© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

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

Sneha Sakharkar*[1], Shubhangi Karnuke[1], Snehal Doifode[1], Vaishnavi Deshmukh[2]

*[1]Department of Computer Science & Engineering, RTMNU/ KDK's Smt. Rajshree Mulak College of Engineering for Women/Nagpur, Maharashtra, India

[2]Assistant Professor, Department Of Computer Science and Engineering, KDK's Smt. Rajshree Mulak College of Engineering for Women/ Nagpur, Maharashtra, India

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, Cloud Computing.

I. 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.

II. EXISTING SYSTEM

Data mining can be a serious threat to the cloud security. Specially to the organizations dealing with

the financial, Government, education or legal issues of people. 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. With the advancement in technology, industry, and research a large amount of data is being generated which is increasing at an exponential rate traditional data storage system are not able to handle data and also analyzing the data becomes a challenge and thus it can not be handle by traditional analytic tools.

Data privacy is one of the major issue while storing the data in a database environment. Data mining based attacks, allows an adversary or an unauthorized user to infer valuable and sensitive information by analyzing the result generated from computation performed on the raw data. It prevents any intermediate data leakage in the process of computation while maintaining the correctness and validity of data mining process.

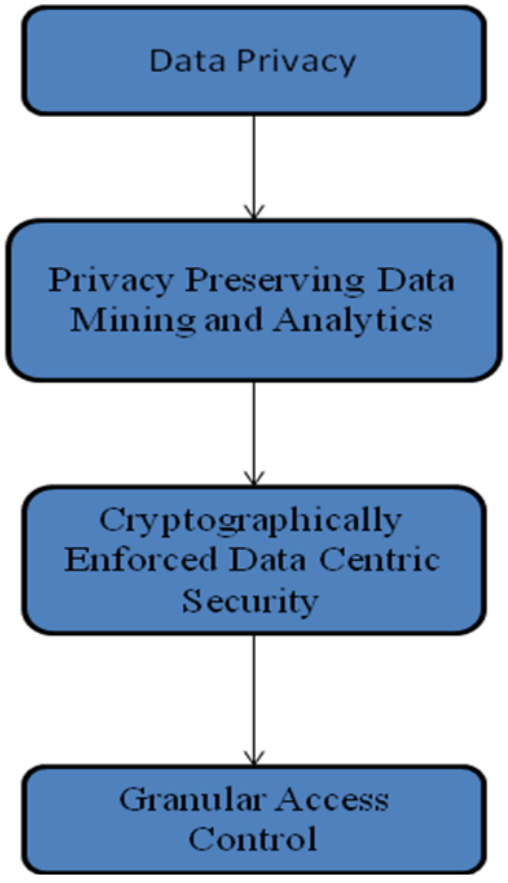

Figure 1. Block Diagram of Data Privacy

III. PROBLEM DEFINITION

To develop a system which will provide security for data mining of cloud using homomorphic encryption as well as RSA Algorithm. The purpose of our research is to enhance the security of the cloud through data mining techniques with specific reference to a system. It is limited to specific cloud computing applications and the research finding make use of a single system. As illustrated in the research, e-commerce websites adopt a cloud server and store multiple frequent data sets related to the clients who visit their websites. They combine their web applications with the cloud services. In addition, they import users data to the cloud and store them in the cloud database. Thereafter, the cloud exports the contents of the database. It was observed that, with the single cache system, the security of the cloud application could be enhanced.

IV. PROPOSED SYSTEM

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 defined as the Homomorphic Encryption allows for the encrypted data to be arbitrarily computed which is a solution that aims to preserve the security, confidentiality and data privacy. This system proposes methods that ensure the confidentiality and privacy

in the mining of databases based on fully homomorphic encryption.

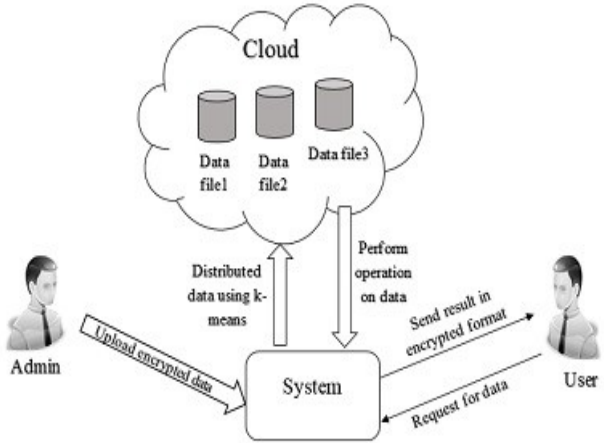

Figure 2. System Architecture of Sender and Receiver Side

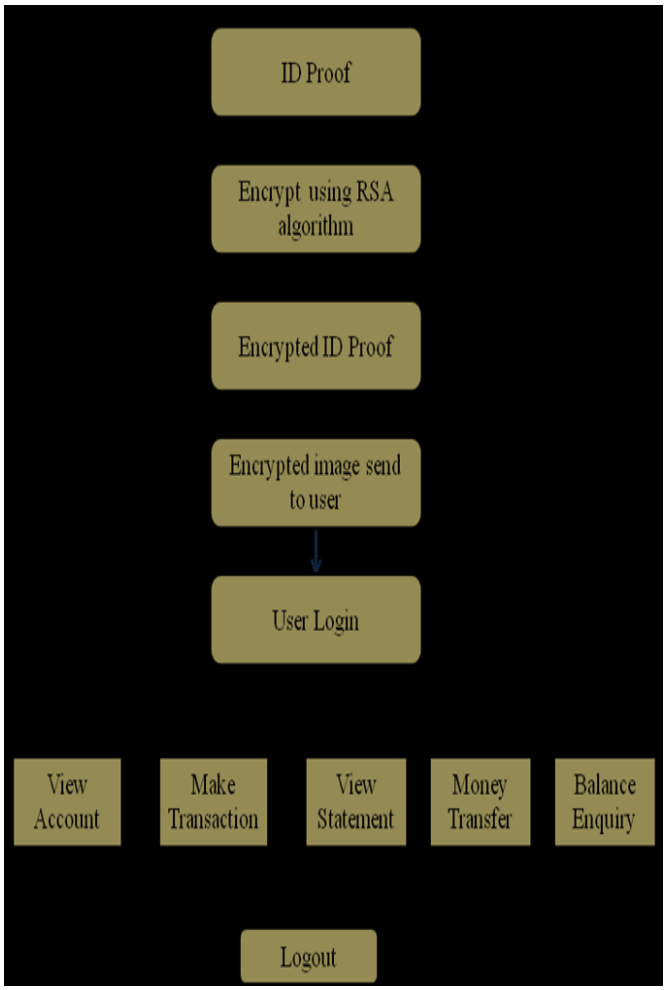

Figure 3. Block Diagram of proposed System

V. RESEARCH METHODOLOGY

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.

RSA (Rivest-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.

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.qand (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}

Encryption-

Step 1: Obtain public key of recipient KU={e,N}

Step 2: Computes: C=M mod N, WHERE 0<M<N

Decryption-

Step 1: Uses their private key KR={d,p,q}

Step 2: Computes: M=C mod N

Figure 4. User Login page

Figure 5. Admin Login page

Figure 6. Admin Approve/Disapprove page

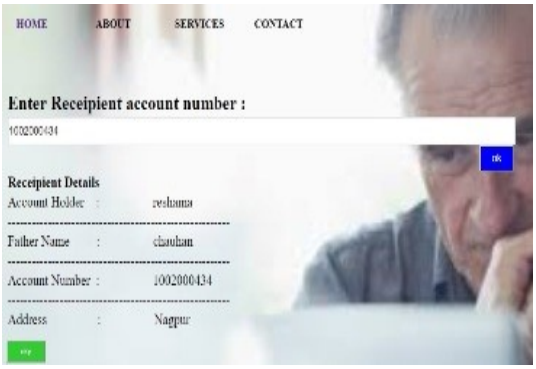

Figure 7. Money Transfer Page

Figure 8. Amount Transfer page

Figure 9. Send OTP page

Figure 10. OTP generation

VI. 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. According to author this method solves the privacy issues of the cloud.

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.

VII. ACKNOWLEDGEMENT

We are thankful to our guide Prof. Vaishnavi J. Deshmukh Associate Professor in Department of Computer Sci. & Engineering for her valuable support. Also we are thankful to the Department for the technical support.

VIII. REFERENCES

[1]. Deepti Mittal, Damandeep Kaur, Ashish Aggarwal, "Secure Data Mining in Cloud using Homomorphic Encryption". IEEE Cloud Security.

[2]. SunandaRavindran , ParsiKalpana,"Data storage security using partially homomorphic Encryption in cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4.

[3]. Hemalatha , Dr. R. Manickachezian, "Performance of ring based fully homomorphic Encryption for securing data in cloud computing", International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, Issue 11, November 2014.

[4]. Mr. V. Biksham , Dr. D. Vasumathi, "Homomorphic encryption applied on cloud", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences (NCDATES- 09th & 10th January 2015).

[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, "A fully homomorphic encryption Implementation on cloud computing", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8 (2014).

[7]. V. Bhagat(2014), "Student Authentication framework in Online Examination Using Visual Cryptography", International Journal For Research In Applied Science And Engineering Technology(IJRASET),Vol. 02, Issue 07, PP.316-319.

Biography

Sneha R. Sakharkar is perceiving her B.E.(Computer Sci. & Engg) from RTMNU-Nagpur University, Her area of interest focus on programming networking, & her research interest on cloud computing & Android Application.

Ms. Snehal V. Doifode is perceiving her B.E.(Computer Sci. & Engg) from RTMNU-Nagpur University, Her area of interest focus on networking, programming , Algorithm & system security

Ms. Shubhangi R. Karnuke is perceiving her B.E.(Computer Sci. & Engg) from RTMNU-Nagpur University, Her area of interest focus on networking, programming & coding.

Ms. Vaishnavi J. Deshmukh received her bachelors and masters degree in Computer Science & Engineering from Amravati University and. She is currently working as an Assistant Professor with the Department of Computer Engineering, Smt. Rajshree Mulak College of Engineering for Women, Nagpur, RTMNU-Nagpur University, India. She has 6 years of teaching experience. Her research interests mainly focused on E-Commerce, IoT, and Image Processing & Computational Photography.