Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy Preserving using Homomorphic Encryption

Mupnesh Kumari
School of Computer Science and Engineering
Bahra University, India

Priyanka Sharma
School of Computer Science and Engineering
Bahra University, India

Abstract— In the recent time, privacy preserving has been studied extensively, because of the extensive explosion of sensitive information. Privacy preserving is one of the important areas that aim to provide security for secret information from unsolicited or unsanctioned disclosure. This has triggered the development of much privacy preserving technique using encryption algorithm.

This work will present the privacy using asymmetric encryption. The field of privacy has seen rapid advance in recent years due to increase in the ability to store data. In asymmetric encryption, RSA and ECC encryption algorithms are used to encrypt the data. In this, the data stored in the database will be encrypted. The data can be encrypted by using the security keys.

The RSA and ECC are used to import the data from the database which is connected to it and encrypt the data by using the keys. A window will be presented on which the output in encrypted form will be shown and the difference between the outputs of the algorithms is also presented.

Our proposed protocol makes use of Homomorphic encryption technique to secure the information.

Keywords— privacy preserving, Homomorphic encryption, Encryption, RSA , ECC.

I. INTRODUCTION

Privacy preserving standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security.

Privacy preserving is an important in order to guard against identity theft. Businesses also need security because they need to protect their trade secrets and proprietary information. Cyber-terrorism is one of the major terrorist threats posed to our nation today. As we have mentioned earlier, this threat is exacerbated by the vast quantities of information now available electronically and on the web.

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers. We use the asymmetric encryption and RSA algorithm, ECC algorithm. RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adlemen. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

Elliptic curve has a rich and beautiful history and mathematicians have studied them for many years. They have been used to solve a various types of problems. The first use of elliptic curve in cryptography parlance was Lenstra's elliptic curve factorization algorithm. Inspired by this sudden unexpected application of elliptic curves in integer factorization, Neal Koblitz and Victor Miller proposed, in the mid-1980s, the elliptic curve public key cryptographic systems. Since then an abundance of research has been published on the security and efficient implementation of elliptic curve cryptography. In the late 1990s, elliptic curve systems started receiving commercial acceptance when accredited standard organizations specified elliptic curve protocols, and private companies included these protocols in their security products.

II. LITERATURE REVIEW

The review of literature reveals that the research communities whose work can contribute to privacy preserving distributed data mining. First discuss privacy preserving work in the data mining community. Then related work from the cryptography and security communities and finally distributed data mining work. Over the past few years, several approaches have been proposed in the context of privacy preserving data mining. Some of the main approaches include heuristic based approach, reconstruction based approach, and cryptographic approach. The underlying concept of the heuristic based approach technique is: how to hide sensitive rules that can be mined from the original data while

maximizing the utility of the released data. In the reconstruction based approach , we first use some methods to distort the values of the original data and then release these distorted data. The third approach is Cryptography based approach which has been developed to solve the following problem: Two or more parties want to conduct a computation based on their private inputs, but neither party is willing to disclose its own output to anybody else. This problem is referred to as the Secure Multiparty Computation (SMC) problem, which requires that no more information be revealed to a participant in the computation than that participant's input and output.

One of the research by (Rakesh Agrawal, Ramakrishna Srikant, in 2000) describes the issue of privacy preserving data mining. Specifically, they consider a scenario in which two parties owning confidential databases wish to run a data mining algorithm on the union of their databases, without revealing any unnecessary information. Our work is motivated by the need to both protect privileged information and enable its use for research or other purposes.

Martin Leslie in 2006 of the project by focussed by elliptic curve cryptography is implemented in the NSA's Suite B, "intended to protect both classified and unclassified national security systems and information" as described in [8], where it used for both digital signatures and key exchange. This shows that elliptic curve crypto is ready for real world use and is to be preferred in many cases over other cryptosystems. We have shown some of the reasons for this in this paper and also seen some of the ways that elliptic curve crypto can be attacked and factors that you need to be careful of in implementation.

The research done by Dr.A.Vinaya Babu,2010 focussed on main objective of data mining is to extract previously unknown patterns from large collection of data. With the rapid growth in hardware, software and networking technology there is outstanding growth in the amount data collection. Organizations collect huge volumes of data from heterogeneous databases which also contain sensitive and private information about and individual .

The researcher Dr. Ramesh Kumar,2012 states that to speed up the implementation of the RSA algorithm during data transmission between different communication networks and Internet, which is calculated to generate the keys by a program prepared in a C # language and then save these values of the keys in the databases created by SQL Server 2008 R2.Privacy is main concern in the present technological phase in the world. Information security has become a critical issue since the information sharing has a common need. Thus privacy is becoming an increasingly important issue in many data mining applications in various fields like medical research, intelligence agencies, hospital records maintenance etc.

Ekta Chauhan , Sonia Vatta in 2013 describes privacy preservation in data mining by using the homomorphic encryption to add security so that any data mining technique does not lose its valuable data and used the asymmetric encryption with RSA encryption. Here, assumed that the decryption occurs entirely at the Server. For real time applications with crucial time-constraints like biomedical applications, the keys for decryption can be distributed to the user for faster decryption and retrieval of data. If client encrypts the data he/she will be able to see it normally but the server or other clients will not be able to see its clear text format.

Seema Kedar, Sneha Dhawale, Wankhade Vaibhav, Pavan Kadam , Siddharth Wani , Pavan Ingale in 2013 privacy preserving data mining techniques are remarkably good, but there is always extent for more enhancements. This survey paper on PPDM can be helpful for finding the loopholes and drawbacks of existing data mining techniques. This survey ensures efficient privacy preserving of data. The use of existing algorithms works towards the direction to reduce the impact of PPDM on the source database.

The study done by Nivetha.P, Thamarai selvi in 2013 explains a brief survey on various standard techniques for privacy preserving data mining was presented namely: randomization, anonymization , secure multiparty computation. Because of the increasing capability to trace and gather large amount of sensitive information, privacy preserving in data mining applications has become an important concern.

One of the researcher Amare Anagaw Ayele1 Dr. Vuda Sreenivasarao, 2013 states that security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption.

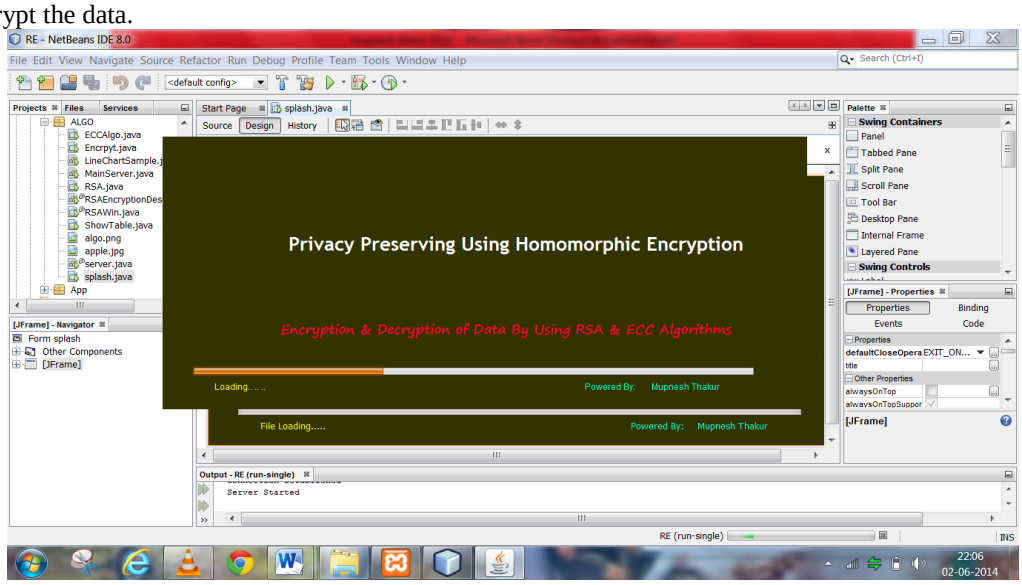
III. OBJECTIVES

The objectives of this project are:

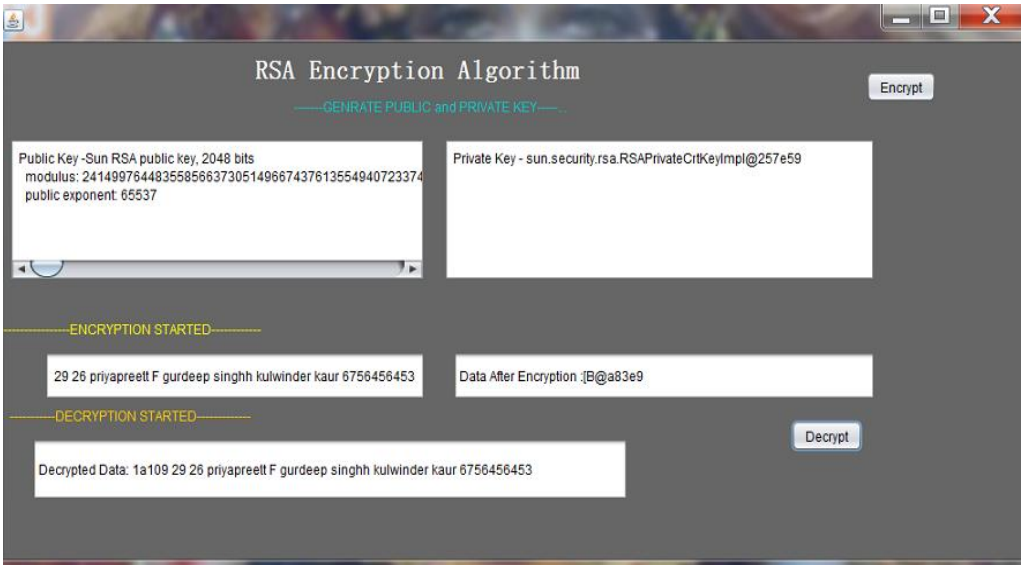
1. Privacy preserving using RSA algorithm.
2. Privacy preserving using ECC algorithm.
3. Comparison of the execution speed of the RSA and ECC algorithms.
4. Comparison of the keys size of RSA and ECC algorithm after encryption.

IV. IMPLEMENTATION AND RESULT

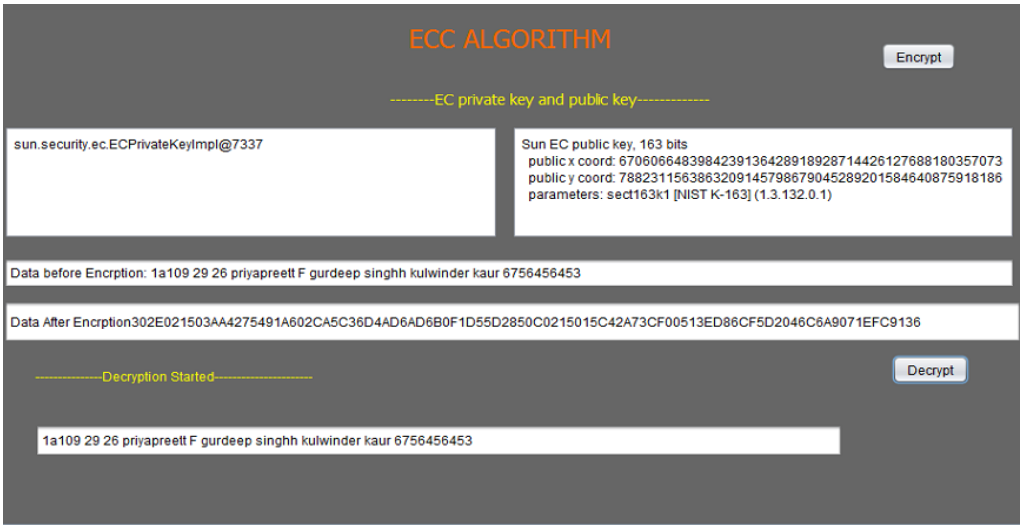
All code for this dissertation was implemented in Java and will describe security by using Homomorphic encryption. Connect xampp to the netbeans where the security code is implemented. From the xampp we import the data and on that data the surety are impelemented. Private and public keys are generated by RSA and ECC algorithms. These security keys are encrypt the data.



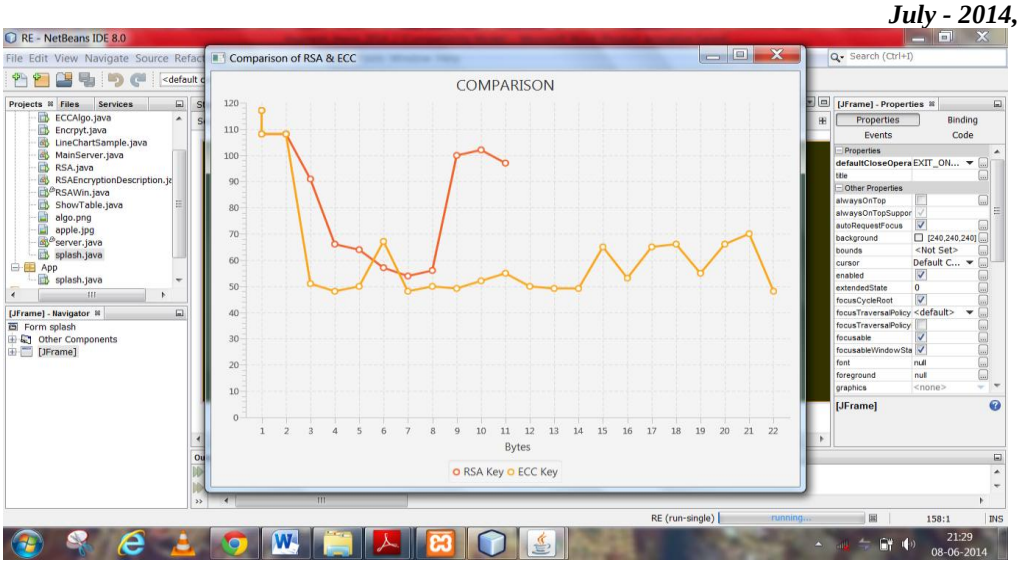
Loading the data



Encryption and Decryption of the data using RSA algorithm



Encryption by using ECC algorithm



Comparison RSA and ECC keys

V. CONCLUSION AND FUTURE SCOPE

Privacy preserving is an on-going research area and there are a lot of issues that needs to be addressed. Security implemented on the data so that no one can access the information is the main issue.

In our approach, we have implemented privacy preservation by using the homomorphic encryption it add security so that any technique does not lose his valuable data. In our approach we are using the techniques on our database by encrypt its value. Here, we also decrypt the data to check that whether same information encrypt or not. For real time applications with crucial time-constraints like biomedical applications, academic's intuition the keys for decryption can be distributed to the user for faster decryption and retrieval of data.

Run one copy of software only on client which import the data from the server. On the server there is database in which data of the student stored are encrypting by using the security keys. So to decrypt properly encrypt and decrypt in same application without any closing.

Future scope: The market for Personal Digital Assistants (PDA) is growing sharply and PDAs are becoming increasingly attractive for commercial transactions. One requirement for further growing of E-commerce with mobile devices is the provision of security. We can implement elliptic curves over binary fields on a Palm OS device.

REFERENCES

[1] Rakesh Agrawal, Tomasz Imieliski, and Arun Swami. Mining association rules. between sets of items in large databases. In Proceedings of the 1993 ACM SIG-MOD international conference on Management of data, 1993.

[2] Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, and J Sander. Lof: Identifying density-based local outliers. In Proceedings of the 2000 ACM SIG-MOD international conference on Management of data, 2000.

[3] Rakesh Agrawal and Ramakrishnan Srikant Fast algorithms for mining association rules in large databases. Proceedings of the 20th International Conference on Very Large Data Bases, VLDB, Santiago, Chile, September 1994.

[4] Wiener, Michael J. (May 1990). "Cryptanalysis of short RSA secret exponents". Information Theory, IEEE Transactions on:

[5] Varun Chandola and Vipin Kumar. Summarization. In Fifth IEEE International Conference on Data Mining, Houston, TX, November 2005.

[6] Eric Eilertson, Levent ErtÄoz, Vipin Kumar, and Kerry Long. Minds a new approach to the information security process. In 24th Army Science Conference.US Army, 2004

[7] Privacy Preserving Data Mining Using Cryptographic Role Based Access Control Approach. Lalanthika Vasudevan , S.E. Deepa Sukanya, N. Aarthi* 2008 Vol I IMECS 2008,.

[8] Anor F.A. Dafa-Alla, Eun Hee Kim, Keun Ho Ryu, *Yong Jun Heo "PRBAC: An Extended Role Based Access Control for Privacy preserving Data mining" In Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science(ICIS'05) of IEEE, 2005 .

[9] Ekta Chauhan , Sonia Vatta Bahra University, Waknaghat *: Cyber Security in data mining using Homomorphic Encryption in Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

