IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

Performance of Asymmetric Homomorphic Encryption Algorithms for Privacy Preservation in Location Based Services

S. Vijaya Lakshmi[1], Gurajala Mounika[2] , Shirisha Kampati[3],

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India [1,3],

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India [2]

ABSTRACT: -Human's need for storing data efficiently is perpetual, when relying on third party services for data storage, whether storing personal or critical data, even though claimed to be completely secure, cannot be trustworthy. During security breaches or situation of personal infringement of the service provider, the need for a mechanism which can be used to protect data from any kind of unauthorized disclosures. There comes the methodology of Homomorphic Encryption. It is an encryption methodology that allows computations to be done on the data without actually seeing the values. In this project, I am using Craig Gentry's scheme which implements Fully Homomorphic Encryption. It is the combination of both AES and paillier encryption algorithms. This project contains GUI designed to fire SQL queries over encrypted data, encrypted using paillier encryption scheme, and perform operations directly over the encrypted text as it would perform directly on plain text. Craig Gentry's scheme is an efficient algorithm than the other algorithms existed for the Homomorphic Encryption because, it gives Fully Homomorphic Encryption in a simpler way and gives fast results than the available Zaryab Khan's Scheme. Craig Gentry's Scheme is Bootstrappable whereas Zaryab Khan's scheme works only where there is less noise.

KEYWORDS: Location-Based Services, Privacy Preservation, Collaborative TTP Free, Privacy Homomorphism.

I. INTRODUCTION

Encryption is a process by which we are able to change our confidential information into aformat which is not understood to computer or human beings, especially to prevent fromexposing the information to unauthorized persons which leads to the destruction of one'sbusiness or privacy. In encryption methodology, plain text is modified using an algorithmwhich will change its form, gives cipher text that can only be read after decryption. The mainpurpose for encrypting electronic data stored in workstation, devices or servers is to ensuresecurity, protection of data, and to secure other digital assets this can be termed as end-to-endencryption, which is useful for safety of data. The Shannon model of cryptography, is one ofthe contemporary models used in cryptology. It ensures security of data. As all data is encryptedinto the system and is never exposed to the outside world. Data can be decrypted and then canbe used, only by authorized users. It is necessary to encrypt data, so that any cyber-attackdoesn't harm the integrity of data. There are some applications where encryption anddecryption of data are considered an overhead, because availability of data is very crucial. Thetime lost in encryption and decryption is not affordable in such cases.

Mostly, the encryption methods are based on symmetric or asymmetricencryption. But Homomorphic Encryption is a different encryption algorithm. It is a methodthrough which anyone will be able to perform mathematical operations over the encrypted datawithout worrying about any loss of the important information because of the computationsdone on the data. It is a property that an encryption method shows when any computation onthe data is done, the algorithm set it into other values, meaning it encrypts it while preservingthe end result. For example, if 25 is stored as 249 in the server and another value 67 is storedas 192 is added or multiplied then answer be 92 stored as 512 and all these computations aredone over encrypted data and changes are stored, when the computed value is decrypted, wouldresult the value that the user would expect.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

Problem Definition

Fully Homomorphic Encryption using Craig Gentry's Scheme which is used for more securityand high confidentiality for Databases. The main aim of this project is it involves encryptionof the whole database including column names. Encrypted data can be manipulated andanalysed without actually being decrypted. We can do computations on encrypted data itselfand the result will affect on encrypted and original data as well. The primary goal ofHomomorphic Encryption is to allow computations on encrypted data. The task is to developa program for GUI cryptosystem using to perform computations on encrypted database itself.The GUI asks the users to enter the user's information like IP address, password, etc., andverifies whether the user is authorized for the database and have the encrypted key. If he hasthe key it will show the encrypted and decrypted data as well. If he doesn't have the key forthe data then only encrypted data will be shown. You can also check in the server that the datacreated will be stored in encrypted format only.

Project Scope

The users of the database can have the privileges like:

- Create a database and tables under that database.
- Create a table of at most 3 columns.
- Insert values into the table.
- Update the information of the database.
- Update the information by performing addition, multiplication the database.
- The encrypted key will be available to the user.
- The data stored in the server will be in encrypted form.
- If others try to access the database, they can only see the encrypted database.
- Other than the owner of the database, others can view the database in encrypted form
- and can perform calculations on the encrypted values without seeing the original values.

Existing System

The current existing cryptosystems are mostly based on SymmetricKey Encryption and Asymmetric Key Encryption. The traditional public keyencryption (Symmetric & Asymmetric) requires the keys to be sent to decrypt the databefore it can be analysed or manipulated. So, third parties are evolved who acts as amiddle-parties who gives security for the data to the customers. Customers should givetheir whole data to the third parties to secure the database. So, we don't give anyconfirmation that data will be secured and the confidentiality and integrity of the datais preserved. Because, we are giving the whole data to others. And also, when we sendthe data to the others it will sent as encrypted and the receiver have to decrypt the datato perform arithmetic operations on the data and will sent back the data to the originaluser. So, the original values are stored in the server in decrypted form and also the otherpersons to whom we can send also can see and know the original values. So, we cannotguarantee the confidentiality, integrity and authentication.

Proposed System:

The proposed system (Cryptosystem for secure computations on databases usingHomomorphic Encryption) is implemented using Homomorphic Encryption which doesn'trequires any trusted third party. Homomorphic Encryption is of three types: PartiallyHomomorphic Encryption where we can perform either multiplication or addition, FullyHomomorphic Encryption is the scheme where we can perform both addition andmultiplications on the databases. We also have Somewhat Homomorphic Encryption which isthe combination of Partially and Fully Homomorphic Encryption.

II. LITERATURE SURVEY

Cryptographic systems can be put to use in any domain, including networks, databases,infrastructure. In this survey, i have discussed the most notable works done in the domain.Gentry introduced "Fully homomorphic encryption scheme", which allows anyone to work onencrypted data without decrypting at any point. A three-step process is done by the authors,beginning with an introduction of encryption scheme which evaluates its own decryption
circuit and calls its bootstrappable.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

Makkaoui et. Al., worked on "hybridizing the homomorphic encryption scheme" tosupport all homomorphic properties. They inspected the possibilities through which algebraicstructures could be used to hybridize the existing schemes which supports limitedhomomorphic properties.

Cheon and Kim, introduced a hybrid homomorphic encryption scheme that combinesPublic Key encryption (PKE) and Somewhat homomorphic encryption (SHE), which reducedthe storage requirements for Homomorphic applications. They concluded that their scheme isuseful in cloud environments where small bandwidth, low bandwidth and efficientcomputations are required.

Sha and Zhu, proposed two methodologies by which they are making RSA algorithmadaptable to fully homomorphic schemes. Method one makes use of Pascal triangle formula toconvert the algorithm to make it fully homomorphic and method two utilizes the moduloarithmetic to convert the legacy RSA algorithm derivation in a form where the resultantalgorithm becomes fully homomorphic.

J. He and Wang studied the application of cryptography over RDBMS which wasevaluated for its security and processing capability of huge data. They introduced the conceptof security dictionary, which is used to store all of the information that is used to manage theobjects in a database, and proposed several secure management methods such as password-basedencryption, public key- based encryption.

Munir proposed a new security model for Database as a Service model which isavailable as a SaaS service from cloud providers. He described a security Architecturecomprising of 4 phases with approaches to implement the required security levels in a cloudenvironment.

III. METHODOLOGY OF CRYPTOSYSTEM FOR SECURECOMPUTATIONS OVER DATABASES USINGHOMOMORPHIC ENCRYPTION

Key based encryption techniques:
In ancient era because calculation was very hard so they prefer to use not lengthy keys inrespect of bits but on the other hand it's safe to use longer key. Communications also one canencrypt in n-bit blocks. It is true that the longer a key is, more difficult for one to break theencrypted message. Encryptions consist of two categories:

- Private Key or Symmetric Key Encryption
- Public Key or Asymmetric Key Encryption

Private Key or Symmetric Key Encryption:
By using symmetric encryption algorithms, data is converted to a form that cannot beunderstood by anyone who does not possess the secret key to decrypt it. Once the intendedrecipient who possesses the key has the message, the algorithm reverses its action so that themessage is returned to its original and understandable form. The secret key that the sender andrecipient that both of them use could be a specific password/code or it can be random string ofletters or numbers that have been generated by a secure random number generator (RNG).There are two types of symmetric encryption algorithms: Block algorithms which encrypts datain the form of blocks. Stream algorithms encrypts data in the form of streams. AES, DES,IDEA, Blowfish, RC5 and RC6 are block ciphers. RC4 is stream cipher.

Fig: Process of Private Key or Symmetric Key Encryption

In Fig, first the plain text is encrypted using Symmetric key and changed to cipher textwhen sender sends to the receiver. After receiver gets the cipher, he decrypts the cipher textusing the same symmetric key and get back the original plain text to perform computations.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

Public Key or Asymmetric Key Encryption:

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that usestwo mathematically related, but not identical, keys - a public key and a private key. Unlikesymmetric key algorithms that rely on one key to both encrypt and decrypt, each key performsa unique function. The public key is used to encrypt and the private key is used to decrypt.Elliptic curve cryptography, RSA, Diffie-Hellman key exchange are some of the Asymmetrickey Encryption algorithms.

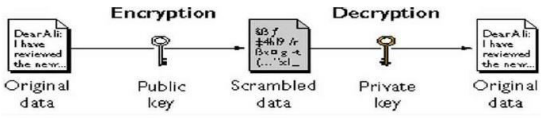

Fig: Process of Public key or Asymmetric key encryption

In Fig, the original data is encrypted using Public key while sender sends the data to theother persons. The cipher text then decrypted using private key by the receiver and gets theoriginal data to perform computations over the data.

IV. RESULTS AND DISCUSSIONS

A cryptosystem for the Homomorphic Encryption is created using Awt and Swings. Tovisualize the working of the encryption scheme, GUI was created which lets user selectdifferent arithmetic operations, which can be performed on the database as shown in figure 2.The GUI lets user execute SQL commands on a database which can be set up on the hostmachine or any remote machine which is in the same network as the host machine. Theapplication when executed creates and stores a private key which is used for encryption anddecryption process, the plaintext entered by the user is replaced by the ciphertext and a SQLquery consisting ciphertext is executed.

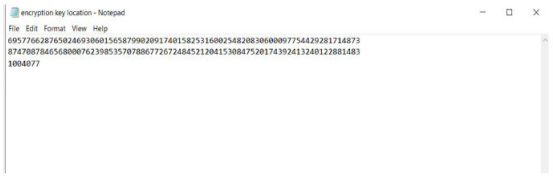

Fig: Encryption key location file with generated key

In Fig, the key will be generated using Homomorphic Encryption and the 512-bit key isstored by creating a file as shown in the figure. The owner can only see the original values ifhe has the key. If he lost the key then he cannot see the original values.

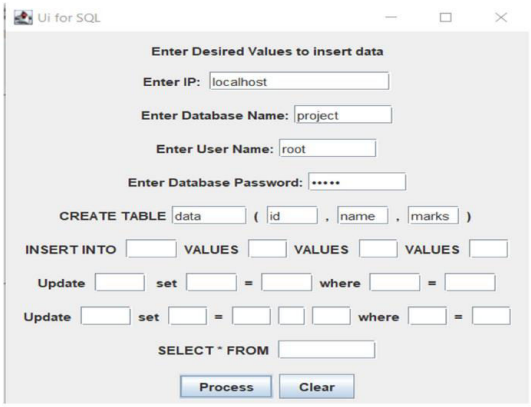

Fig: Output of GUI for asking user to enter details and data.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

Fig shows the GUI output window which allows to authenticate himself by entering the IPaddress and database name, user name, password and then queries like create table, insertvalues, update values and other update query for computation. The process button gives theencrypted and decrypted view of the data. The clear button clears the data entered in the GUIwindow and allows the user to re-enter again. This includes by adding buttons and other options using Awt and Swings.

The key will be created and used for the visibility of the original values. If the key is lost thenthe encrypted table will be shown. If the details are not authorized then error will occur and ifwe press the process button, nothing will happen we just get the error. To give the authority ondatabases the owner should write the query for giving authority to the other person using hisIP address.

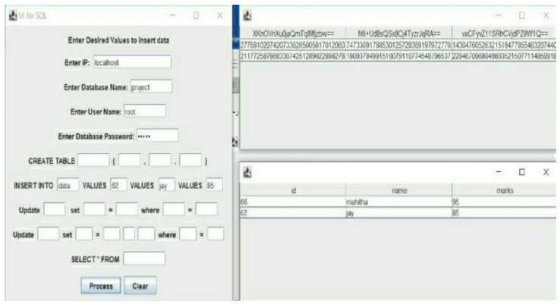

Fig: Insert query operation showing encrypted and decrypted tables.

This Fig shows the insert query operation to insert three column values id, name, marksand shows the corresponding encrypted and decrypted tables.

V. CONCLUSION AND FUTURE SCOPE

Conclusion:

Through this project, it has been shown how the encrypted data can be passed over todatabases which is present locally or remotely. Also, the result showcased HomomorphicProperty of the Encryption Algorithm by doing different operations over the encrypted datalike performing arithmetic operations +, -, * etc. It provides a method that would help in makinga system where the data can be stored encrypted and operations can be done on the encrypteddata and the value decrypted would retain the same value as expected if the operations wereperformed on plain text. In this System the Database used is entirely encrypted that the Columnnames and database name is even encrypted at the time of creation using RSA algorithm. Whichmeans that any modification done on the Database is unknown to anyone how tries to attack itas any data regarding tuple values or database is unknown.

Future Scope:

Throughout this project, the length of the cipher text is considered too large to be usedwith ordinary Java data types, so the code should be modified to produce smaller cipher textlength. So, the Algorithm can be further synthesized to generate lesser length of the ciphervalue for better memory management. This System currently, is not smart enough to relateappropriate Encryption and Decryption function as per the input data type. Once done, it canbe tested and deployed over to a Cloud Environment. Generic Encryption and Decryptionfunction can be created to accept any data value and can encrypt and decrypt it. The Encryptionmethodology discussed in this paper can be programmed to handle further mathematicaloperations like exponents, modulo etc. The Encryption method discussed in this paper onlyprovides security from other authorized / unauthorized people not able to see the original data.But doesn't prevent any unauthorized operations thus corrupting the data. In order to preventthe encrypted data being hampered or corrupted we must have to employ mechanism likeHamming Code, Parity Bits, Checksums, Cyclic redundancy checks (CRCs), Cryptographichash functions etc. that ensure data integrity to prevent unauthorized people from hamperingthe data. We can also develop an application so that the data is stored and people can send toothers using that application, so that the others can receive the data and perform computationson the encrypted data.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004096

REFERENCES

[1] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphism.Foundations of Secure Computation, pages 168–177, 1978 5. Stepanov M., Bezzateev S., JungT.C. Privacy Homomorphism for Delegation of the Computations.

[2] M. Yokoo, K. Suzuki. Secure Multi-agent Dynamic Programming based on HomomorphicEncryption and its Application to Combinatorial Auctions, Proceedings of the FirstInternational joint Conference on Autonomous Agents and Multiagent systems (AAMAS),2002:112-119.

[3] Kumari, Sarita. "A Research Paper on Cryptography Encryption and CompressionTechniques." International Journal of Engineering and Computer Science, 4 Apr. 2017, pp.20915–20919., doi:10.18535/ijecs/v6i4.20

[4] Joshi, Mukund R., and Renuka Avinash Karkade. "Network Security with Cryptography."International Journal of Computer Science and Mobile Computing, Vol. 4, no. 1, Jan. 2015,pp. 201–204.

[5] Gentry, Craig. "Fully Homomorphic Encryption Using Ideal Lattices." Proceedings of the41st Annual ACM Symposium on Symposium on Theory of Computing - STOC '09, 2009,doi:10.1145/1536414.1536440.

[6] Makkaoui, Khalid El, et al. "Can Hybrid Homomorphic Encryption Schemes Be Practical?"2016 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016,doi:10.1109/icmcs.2016.7905580.

[7] Cheon, Jung Hee, and Jinsu Kim. "A Hybrid Scheme of Public-Key Encryption andSomewhat Homomorphic Encryption." IEEE Transactions on Information Forensics andSecurity, vol. 10, no. 5, 2015, pp. 1052–1063., doi:10.1109/tifs.2015.2398359.

[8] Song, Xidan, and Yulin Wang. "Homomorphic Cloud Computing Scheme Based on HybridHomomorphic Encryption." 2017 3rd IEEE International Conference on Computer andCommunications (ICCC), 2017, doi:10.1109/compcomm.2017.8322975.

[9] Sha, P., & Zhu, Z. (2016). The modification of RSA algorithm to adapt fully homomorphicencryption algorithm in cloud computing. 2016 4th International Conference on CloudComputing and Intelligence Systems (CCIS).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details