Data Confidentiality in Cloud using Multi-party Computation

A.Vijaya Kumar, P. Ramya, R. Poojitha, M. Lahari

Abstract: - A new era has approached where we are storing our information in cloud and performing several computations on powerful servers remotely. In cloud, data is not completely secured and sometimes under the control of untrusted Third parties. Some secured protocols are being implemented. The secure multi-party computation protocol, which is existing, demands the inputs to be encrypted using a public key. So, these reasons limit this Secure Multi-party computation to be employed. In the current paper, we put forward a protocol named homomorphic encryption where the input function is being encrypted by different key. This paper also uses Multi-party computation which is one of the most secured technique in cryptography.

Keywords: - Cloud Computing, Confidentiality, Multi-party computation, Homomorphic encryption.

I. INTRODUCTION

Data Confidentiality can be achieved through Secure Multiparty Computation [1] [2] [3] [4] [5] [6] [7] [8] [9] [11] and Homomorphic Encryption. In Secure Multiparty Computation a joint computation function is being performed on the given inputs by taking it from the users where as in this data cannot be completely secured and this can achieved through Homomorphic Encryption [1] [3] [4] [5] [6] [13] [14] [15] by not asking the inputs and computations will be performed on the encrypted data as if they were performing on the original data and for that we used Paillier Algorithm for better security purpose.In section II, the preliminaries i.e., Secure Multi-party Computation and Homomorphic Encryption terms are discussed. In section III, the work related to this paper/Literature survey is mentioned. The methodology proposed is in section IV. The results are mentioned in section V. The applications of the proposed methodology are mentioned in section VI. The conclusion and future work are in section VII and VIII respectively.

II. PRELIMINARIES

(A) Secure Multi-party Computation:

Secure multiparty computation is also named as multiparty computation, privacy preserving and secure computation which is also the field in cryptography that also to compute a joint function on the inputs provided to us.

Secure MPC makes us to work and analyze the information for the welfare of the people without revealing the private information which is very confidential.

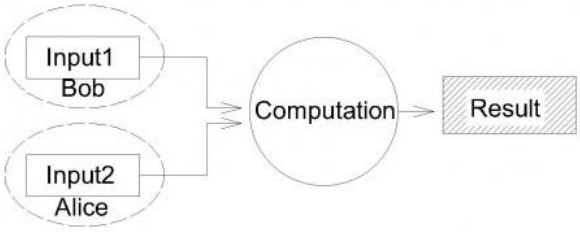

Fig: Multi-party Computation

So as to comprehend what the careful meaning of SMC (secure multiparty calculation) is, we should ready to think about Shamir's Secret Sharing calculation. This algorithm tells us to divide and distribute one value which should be secret to the users. In order to retrieve that available secret value, a smaller number of users must combine their data together. This type of algorithm that is Shamir's algorithm, also used to carry out computations on the secretly shared number. Here, without using a number, we can replace secret as user's personal data. Secure Multi Party Computation also perform the task in the same way as Shamir's algorithm, thus by dividing the user's data into many smaller parts, and the data which is encrypted is sent to a different server. For example, a group of people with their information that is to be stored in cloud needed to be secured before itself, so they jointly compute a function on all their inputs:

- Give a function for X: b1, Y: b2, Z: b3 on which we are going work or compute jointly
- These outputs a 3-tuple: (k1(b1, b2, b3), k2(b1, b2, b3), k3(b1, b2, b3))
- Most of the times all the k1, k2, k3 may not be necessarily same.
- Always people wish to preserve some security properties.
- This security either must be provided either by the adversarial behavior of the participants or by the third party.

(B) Homomorphic Encryption:

This is the process of changing the information or the data into the ciphertext that can be viewed and also we can work on it as if it as a original information which is not actually provided by the

Revised Manuscript Received on January 05, 2020.

***** Correspondence Author

Mr. A. Vijaya kumar, Associate Professor, CSE Department, KL University, Guntur, Andhra Pradesh, India.

P. Ramya, Computer Science and Engineering, KL University, Guntur, AndhraPradesh ,India.

R.Poojitha, Computer Science and Engineering, KL University, Guntur, Andhra Pradesh ,India.

M.Lahari, Computer Science and Engineering, KL University, Guntur, Andhra Pradesh ,India.

user and also the encrypted one. On the encrypted data we can perform the computations without compromising as on the original data.What the homomorphic encryption is changing the form of information or data into another while keeping the same relationships among the data elements in either of the data sets.In Homomorphic encryption confounded numerical tasks are performed on the scrambled information. In distributed computing Homomorphic encryption plays a significant role.

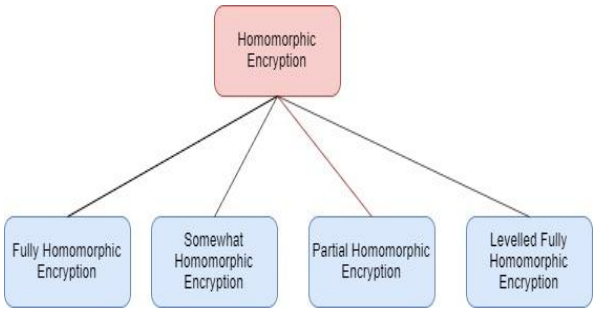

Fig: Types of Homomorphic Encryption

Here we will explain a easy example in what way a homomorphic encryption uses cloud computing in performing operations.

• Let us consider a business XYZ, which is extremely occupied, so it asks cloud supplier to execute the activity. As we realize that lone a cloud supplier will just have the entrance to the encoded set, Finds the distinction of 30-20 and offers the response as 10.

A small example to describe this is:

• An organization named Creta has a very crucial information of data sets which has numbers of 10 and 20. To encrypt this it multiplies each element in it with 3, which creates a new set as 30 and 60.

• Later it sends the encrypted data to cloud. A few months later the other party contacts the Creta and requests for the data.

• As the Creta is busy with their own work it asks the cloud provider to perform the operation which only has the access of encrypted data find the sum as 90 and returns the answer.

• Then the Creta decrypts the data and provides 30 as the output to the other party.

• Hence with this security has been provided to the data.

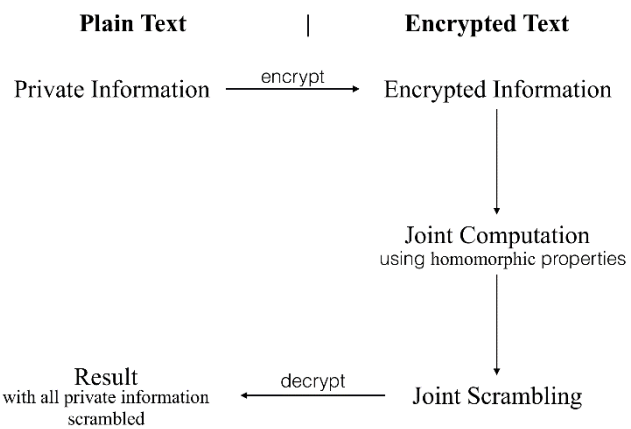

Fig: Homomorphic Encryption

III. RELATED WORK

(A) RELATED WORK OF SEGMENTATION:

Debasis Das et al [1] To store the vast amount data these days a great infrastructure is needed that provides the support for the storage and processing of the data. This is becoming a great challenge for all large MNC's and also for various other sectors to keep their data. Hence Cloud Computing provides the on-demand access and also very much convenient in sharing the resources. So, the MNC's or other organizations tie-up with the cloud and use all the available resources properly. Cloud platform extracts and analyze the useful data from big data. Concerns of cloud computing are confidentiality and privacy. The arrangement is to send the encoded information to the cloud server. Regardless we need to help the valuable estimations on figured information and FHE in supporting manner. Note that mechanisms other than this exists for secure computation, which require diff data providers for exchange of data.The fully homomorphic encryption is better to adapt to the scenario in which we have a lot of data resources. SMPC gives the correct output to everyone for the joint computation not else about anyone info, the users which are performing the calculations may be actively malicious. SMPC can be done by the arbitrary calculations and more number for parties In this way, we can see the SMPC conventions with the goal that the compilers will take input details for mapping, yield is the convention that computes the capacity all the more safely. SMPC gives both privacy and honesty which can be superior to FHE and the confirmed figuring. Security to the information is given by utilizing the cushioning idea called as Optimal Asymmetric Encryption Padding(OAEP) alongside the Hybrid encryption calculation that relies upon RSA to enable the numerous individuals to give the security to their information by utilizing one joint register work on them and it additionally gives the Integrity and Confidentiality to the information. Cryptographic procedures here are Homomorphic encryption and the safe multiparty Computation. OAEP is a Feistel Network. It is a productive cryptographic strategy for cushioning multi

party information without figuring it. Weaves information is scrambled by utilizing a plan called cushioning called Optimal Asymmetric Encryption Padding Combine with the Hybrid encryption Algorithm which depends on RSA. Emily Shen et al. [2] Analysts attempt to make secure multiparty calculation—that takes numerous contributions of information from various gatherings and together figures a capacity combinedly and keep the sources of info mystery. "Data sharing ought to be directed in an exceedingly way that ensures the security and common freedoms of individuals, that jelly business classification, that shields the information being shared, which secures the capacity of the Government to watch, explore, avert, and answer to digital dangers." Trying to accomplish

greater security to the information use SMC. Cryptographers has been making a decent attempt to build up this kind of innovation, called as secure multiparty calculation for three decades. Secure Multi party calculation adjusts that every one of them get familiar with the accurate yield of the joint calculation however nothing else about different data sources. indeed, even the dynamic execution of calculation by a portion of the clients. Secure Multi party calculation would be accomplished for various calculations and for various gatherings. Along these lines, we can see the safe SPC conventions as like of compilers which accepts contribution as detail of the capacity and yield will figures the capacity safely. So as to perceive how it fills in as of compilers let us take a procedure which is called mystery sharing .A m-of - n mystery sharing plan separates a mystery contribution to k number of pieces which are held by various individuals such that m number of individuals can consolidate their offers to recreate the mystery. For instance, you need to make a 2 of 3 mystery sharing plan utilizing the lines in 2-dimensional space. So as to share the mystery s sum three unique individuals, we will pick an arbitrary line. In this y-blocks equivalent to mystery s. Each individual would share their s, which are various focuses on hold. For any two points that diversely characterize a line, an any 2 individuals join to register the mystery key, conversely a solitary offer doesn't uncover anything about mystery key. This sort of procedure can be summed up to ant=y m utilizing the level of polynomials m-1. On the off chance that any two privileged insights p and r have shared, at that point individuals can compute portions of the total p+r by disentangling including their offer together. Portions of the item can likewise be processed p*r through entangled control of the portions of p and r. In the specific situation, a couple of number of structures are additionally accessible for secure MPC advancement of programming, which require little measure of information on the cryptography. This can be empowered by a designer to give a functionals examine of the significant level wanted calculation. through an exceptional language, alongside the accessible explanations that are accommodating which the given information is allowed so as to uncover. These sort of programming instruments can isolate the errands of programming specialists and cryptographers, streamline their association so as to improve ease of use that likewise diminishes the time being developed. Andriana Lopez Alt et al. [3] In on the fly MPC, each client is included on the underlying phase of transferring his/her encoded information to the cloud server and in conclusive outcome in the decoding stage the outcomes are uncovered. Multifaceted nature of both is free on the capacity that is being processed to the complete number of individuals in the framework. Clients ought to choose which capacity ought to be registered in the further or who they have to figure with. They additionally need the identified with past endorse that in the end pick capacities and the capacities by which information is assessed. As we realize that the cloud offers increasingly number of preferences in both cost just as usefulness, it likewise bring up issues of privacy, since put away information can be helpless against snooping either by the cloud supplier or by other cloud suppliers in the cloud. Everybody realizes that the data contains the most touchy information, it is basic for the clients to store the information in the wake of encoding as it were. FHE is the calculation which is reasonable in the setting time where it includes a solitary or significantly more clients, on the grounds that the data sources ought to be encoded under a similar kind of key. All the more ever, there are numerous circumstances where numerous clients, Who have just moved their huge information to store in the cloud in figure structure, and afterward need to choose to fathom joint elements of their information. For instance, They can wish cloud to process the joint factual data all alone information bases, to find the most widely recognized documents in their record assortments, Which runs a calculations part dependent on their post information to arrive at goal or when all is said in done, in the challenge where more clients would need to consolidate their data so as to achieve a most shared objective. Finally, another type of completely homomorphic encryption that they call a multi key FHE which allows a calculation on the data scrambled under the more noteworthy number of disconnected keys As there are increasingly number of clients engaged with any of the calculation or figuring in the arrangement must be limited, as that the all out number of clients in the framework is random.Min Zhao et al. [4] The efficiency of different algorithms are compared based on their security characteristics. These are single homomorphic algorithms. These algorithms differ in many ways based on which homomorphism they perform. Different types of five fully homomorphic encryption algorithms are researched to find out the performance of those algorithms based on security. From this paper we can be able to know which algorithm will provide high security to the data. The GM Algorithm [4] is based on quadratic residue with semantic security and it satisfies only addition homomorphism and it has low efficiency. The GM algorithm is introduced in 1984. In 1985 The ELGAMAL algorithm is introduced to provide the security for data. This calculation depends on open key cryptosystem and elliptic bend cryptosystem and it fulfills any multiplicative homomorphism and can be utilized for encryption. The Hill figure calculation fulfills expansion homomorphism. The RSA calculation depends on number hypothesis and it fulfills any duplication homomorphism encryption. In 1994, a calculation called Improved probabilistic encryption calculation is presented. It encodes n bits of information at once yet can just play out a limited number of expansion homomorphism activity. Paillier encryption algorithm is based on a quadratic residue and it can perform any additive homomorphic operation. At a low possible cost, the confidentiality of data will be guaranteed. The technique used is depends upon encryption scheme called Bulk Copy Scheme. Because of untrusted third parties, this new technique is implemented for outsourcing the secured data and apt to the purpose of Secure multiparty Computation. The data is encoded with many different public keys. There is no interaction of users in this scheme. This scheme provides more security in applications like face recognition with feasibility.

IV. OUR CONTRIBUTION

Paillier Cryptosystem is at first delineated in a very 1999 paper by Pascal Paillier, that outlines associate degree uneven non-deterministic cryptography algorithmic rule with homomorphic additive properties. The cryptosystem additionally provides detached signatures, however not inline signatures as provided by RSA.

Paillier Key cryptography is one of the homomorphic algorithms. The clients who utilize this calculation will have an open key and a private key. The information is first scrambled with the open key and send to the recipient. Then the receiver will decrypt the data with his private key. Paillier key cryptography provides "additive homomorphism".

For example, Bob is the sender and Alice is the recipient. Bob has two messages that are encoded with receiver's public key. Bob add the messages together and will send to receiver. Alice decodes the data with his private key and get the result as the sum of both messages.

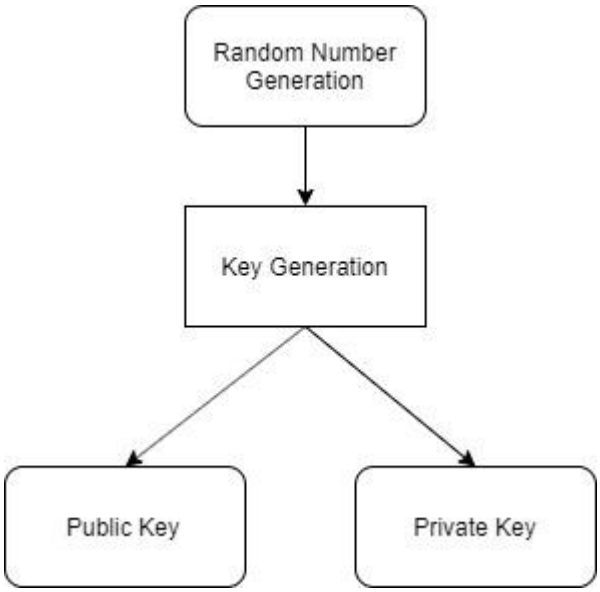

Fig: Paillier Cryptosystem

Example: Casting a ballot System

We need to engrave all polling forms for a political decision board hence outsiders can't check the votes

We need the political race board to have the option to tell who won the political decision

We don't wish the political race board to illuminate us that voter casted a ballot that up-and-comer

With antiquated cryptography and coding there's no methodology for the political decision board to get a handle on who won the political decision while not decoding each vote.

The voting system can be again designed by using additive homomorphism as pursues:

Voters scramble their polling forms with the political race board's open key

Voters send their scrambled polling forms to an examining server

The exploring server includes every one of the polling forms along and sends them to the political race board

The political race board decodes the voting form all out, reports who won the political race while not regularly perusing a voter's voting form.

IV. RESULTS

Public Key(n,g)	(1763,59)	(667,135)
Private Key(lambda,mu)	(103,840)	(280,308)
Message (m)	10	15
Encrypt(m)	2414446	355449
Message(m1)	12	12
Cipher(m1)	197550	271519
Ciphertotal	408898	51594
Result (Decryption of ciphertotal)	22	27

DISCUSSION OF RESULTS:

The data confidentiality is achieved as the receiver get the ciphertotal i.e., the combined result of inputs and decrypts it. The receiver don't know the multiple inputs. The data is secure and cannot be modified.

VI. APPLICATIONS

A. Electronic voting:

In Electronic voting, The people had to cast their vote individually without disclosing to whom they vote to other people. Here, while they cast their votes, they encrypt the vote. So that it is not known to anyone to whom they vote. But, these votes are collected by Election commission to know how many people casted their votes. Then election commission will have the product of the votes casted by the people. They will decrypt that data and acquire results to know how many of the people of the total population casted their votes. People may not be able to know to whom others voted to.

B. Electronic cash:

A new notion is feature of self blinding. The flexibility to alter one coded text into another while not dynamically the content of the decrypting. This application is useful where there is no need of vendors in a shop to pay the amount through our credit card. This application is similar to

e-voting. The goal of both the applications is same. We can purchase the items online without disclosing our details and promoting the notion of e-cash.

VII. CONCLUSION

In this paper, Data in cloud will be secured based on confidentiality. In real world, any third party is not trusted to store and secure the data in cloud. There are many homomorphic encryption algorithms which had provided security but not to full extent. There are algorithms with some disadvantages like Hill Cipher i.e., It is symmetric encryption algorithm and data will be easily decrypted. So, paillier algorithm is better to implement to this approach. This method is only implemented for digits but in future it can be extended for strings and images.

REFERENCES

1. Debasis Das, Department of Computer Science and Information System, BTIS Pilani, Secure Cloud Computing Algorithm Using Homomorphic Encryption and Multi-Party Computation
2. Emily Shen, Mayank Varia and Robert K Cunningham, W. Konard Vesey Cryptographically Secure Computation. 0018-9162 / 15/$31 .00 2015 E E E
3. Adriana Lopez - Alt,Eran Tromer, Vinod Vaikuntanantham, On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption
4. Min Ahao, Yang Geng, Homomorphic Technology for cloud computing
5. Yuangang Yao, Jinxia Wel, JianyiLiu, Ru Zhang, efficiently secure multipart computation based on Homomorphic Encryption Proceedings of CCIS201
6. Ivan Damgard, Valerio Pastro, Nigel Smart and Sarah Zakarias. Multiparty Computation from Somewhat Homomorphic Encryption . R. Safavi. Naini and R.Canetti (Eds.): CRYPTO 2-12,LNCS 7412,pp.643-662,2012.International Association for Cryptologic Research 2012
7. Valtteri Niemi, Ari Renvall. Secure multiparty computation without computers. Theoretical Computer Science 19.1(1998) 173-183
8. Alfredo cuzzocrea, Elissa Bernito. Privacy Preserving OLAP over Distributed XML Data:A Theoretically-Sound Secure Multiparty-computation Approach. Journal of Computer and System Sciences 77(2011)965-987
9. Marcm Andrybowicz, Stefan Dziembowski. Daniel Malinowski, Lukasx Mazurek.Secure multiparty Computation on Bitcoin,2014 IEEE Symposium on security and privacy.
10. Ronald Cramer, Vanesa Daza Ignacio Gracia, Jorge Jimenez Urroz, Gregor Leader, Jaume Martin-Frame and Carles Pardo. On codes, Matriods and secure Multiparty Computation from Linear Secret -Sharing Schemes, IEEE TRANSACTIONS ON INFORMATION THEOREY, VOL. 54, NO.6, JUNE 2008.
11. Andreas Peter, Erik Tews and Stefam Katzenbessier. Efficiently Outourcing Multiparty Computation
12. Under Multikey Keys, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL 8, NO. 12, DECEMBER 2013
13. Ivan Damgard, Martin Geisler and Mikkel Kreigard Homomorphic encyption and secure compasion.
14. Andrea B.Alexandru Student Member,IEEE Konstantinos Gatsis, Member, IEEE, Yasser Sboukry, Member, IEEE, Sanjit A. Seshai, Fellow, IEEE, Paulo Tabula, Fellow, IEEE and George J,Pappas,Fellow, IEEE.Cloud-Based Quadratic Optimization with Partially Homomorphic Encyption.
15. Jean Lousis Raissro, Gwangbae Choi Sylvain pradwevand Raphal Colsenet, Natlle Jacquernot, Nicolas Rosat, Vincet Mooser, and Jean-Prierre hulxux Protecting Privacy and Security of Geonomic Data in i2b2 with Homomorphic Encryption and Differential Privacy

AUTHORS PROFILE

Mr. A. Vijaya Kumar, Associate Professor, CSE Department, KL University. Email: vijay.cse@kluniversity.in

P. Ramya, CSE Department, K L University, Email: ramyapotru459@gmail.com

R. Poojitha, CSE Department, K L University,
Email: pujithaaravipati@gmail.com

M. Lahari, CSE Department, K L University, Email: laharimarella21@gmail.com