ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2019; 5(4): 66-69
www.allresearchjournal.com
Received: 01-02-2019
Accepted: 03-03-2019

Secure multiparty computation for public cloud

Varsha Shingade, Yugalee Patil, Apoorva Patil, Harshada Patange and Dr. Dhananjay Dakhane

Varsha Shingade
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Yugalee Patil
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Apoorva Patil
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Harshada Patange
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Dr. Dhananjay Dakhane
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Correspondence
Dr. Dhananjay Dakhane
Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra, India

Abstract
Cloud Computing is a paradigm shift from the distributed computing where an organization uses resources “as service”. However, users of the cloud are worrying about the privacy of their data that has been supplied to the cloud provider. The solutions to these problems can be provided by the protocols of the Secured Multiparty Cloud Computing (SMCC). Secure Multiparty Computation (SMC) is a paradigm that keeps data of individual parties as secret and provides the private data for computation to evaluate some function of their common interest. The outcome of the computation is made available to all the parties. In this report, we propose SMC solution techniques that can be embedded while designing architecture of cloud computing especially when multiple users of cloud jointly compute some function of their private data inputs. With our experience of developing protocols and devising algorithms for SMC problem we anticipate a crucial role of SMC in cloud computing. In this report, we also explore scenario while discussing various protocols of SMC and their application, with the design of SMC Architecture.

Keywords: Cloud computing, secured multiparty cloud computing

1. Introduction

Organizations uses the data available with them for the different services and makes a better decisions. But sometimes, these benefits do not come without a cost. The society which have the information have seen the emergence of problems like mass manipulation, large scale data breaches and mass surveillance. A post titled ‘Crypto is Dead; Long Live Crypto’ describes that by using traditional methods of cryptography such as encryption and authentication an ultimate solution cannot be obtained. This is because whatever data is present it has to be processed at some point and as we do not have the knowledge that how effectively the operation with be performed we to decrypt all the data that is been encrypted. Moreover there is increase of threats it is not reasonable to assume that some of the attacker may have the decryption key inside the security parameter. An alternative way of addressing such issues is secure multiparty computation (SMC) [3]. SMC allows multiple parties to perform operation on the data which is in the encrypted form and gives the result which is private and thus ensures data integrity and the correctness of the output is guaranteed. The parties present are mutually distrustful, but SMC allows them to perform computation by keeping the data confidential. Thus in other words SMC provides data sharing and data ownership.

Section II describes the literature survey which contains comparisons of various previous research papers. Section III describes the Proposed Technology. Section IV describes the Implementation. Section V describes the Conclusion.

2. Literature Survey

1. Cloud computing security challenges and solutions

Cloud Computing is a set of IT services that are provided to the customer over the network which are owned and delivered by a third party. As the emergence of cloud computing, all types of companies started using their own private cloud to reduce the cost spent on the hardware. Companies like Google, IBM, and Amazon many more large scale industries started using this platform to store and compute their data. As use of this platform has been increasing day by day, then the security issues involved with cloud computing has become a major research topic.

The security of cloud and communication systems becomes a major issue as society becomes increasingly dependent on the cloud computing technology. Cloud computing represents the new evolution in the field of technology which has many demanding security concerns at every level, e.g., network, host, application, and data levels. Breaches of confidentiality, data corruption, man-in-the-middle attack are some of the risk issues related to cloud security. Cloud computing involves communication between client and server through a network. Large amount of time has been consumed to transfer big volumes of data through the network. This becomes a major concern for data-sensitive applications in cloud computing. There are various security issues arises when data has been intercepted over the channel between client and server [6]. Some of them are listed below:

- Breaches of confidentiality
- Potential loss of control/ownership of data
- Account hijacking
- Data Security
- Unauthorized secondary usage
- Network security.

2. Review on Security Management in Cloud computing

Cloud computing is a very easy method through which we can get access to shared pool of resources, which can be configured and released with minimal effort. Cloud security is one of the major challenges in cloud computing. One of the efficient way to secure data on cloud is using different types of encryption algorithms. The key is used to encrypt the data. The encryption and decryption of the user data is done through the same key values. This type of algorithms can be termed as cryptographic algorithms. There are a lot of cryptographic algorithms available, which can be used for security purposes. Some of them are:

Rivest- Shamir- Adleman (RSA)

This algorithm performs the encryption with two random numbers to create the needed public keys and private keys. The keys are used for encrypting the data at the sender's side and decrypting the data at the receivers' side. Sender encrypts the message which is required to be sent across the channel using the receiver's public key and when the message arrives at the receiver's side, the receiver can decrypt the encrypted message using their separately generated private keys [6].

Data Encryption Standrad (DES)

DES is a symmetric-key method of message encryption. Private key is used to encrypt and decrypt the data. This private key must be known to both the sender as well as receiver. DES encryption method is block cipher technique. In this technique blocks of data consisting of 64 bits can be encrypted and decrypted by using a 64 bit key [7].

Advanced Encryption Standard (AES)

AES algorithm has a huge advantage over the rest of the algorithms, it can be used to support any data of multiple combinations (128 bits). And the keys used in this technique are of various lengths (128, 192, and 256 bits). The security process in AES system involves 10 rounds for 128-bit keys initially, and then it has to go through 12 rounds for 192-bit keys, and lastly 14 rounds for 256-bit keys in order to obtain the final encrypted text or to get back the original plain text, that is the initial message. AES allows data length of size 128 bits that can be split into four operational blocks. The output has to go through nine rounds and during each of these nine round it has to go through four transformation [7].

- Substitution of bytes
- Shifting of rows
- Mixing of columns
- Addition of round key.

Based on the review it is found that AES is the most efficient in terms of speed, time, avalanche effect and throughput.

3. Security in Cloud Computing using AES & DES.

Here we have study disadvantages and advantages of AES & DES.

DES

Advantages: The Avalanche Effect is the major advantage which states that a slight change in character or bit will have a drastic change in the cipher.

Disadvantages: Memory Requirement and Simulation Time is more in case of DES [7].

AES

Advantages: - It provides strong security from the attackers and threats. But as the years passed the attack was less and the only attack found was Brute Force attack.

Disadvantages: - The major drawback is that it could not withstand with the attacks like Brute Force, Linear crypt Analysis, because during its design this attack wasn't invented [7].

4. Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud

In today's world there is large number of companies present which have their own private data. Cryptography can be useful for integration of cloud computing. But the problem is data owners cannot fully trust the cloud computing for safe and secure storage. Sometimes the cloud computing could expose the privacy of user data by having unauthorized access to it. For overcoming the above problems, cryptography has been widely applied to ensure data security, privacy and trust in cloud computing [6]. There are 2 types of algorithms:

Symmetric key algorithms

a) Advanced Encryption Standard (AES)
b) Data Encryption Standard (DES)
c) Blowfish Algorithm

Asymmetric Key Algorithms:

a) RSA Cryptosystem
b) Diffie-Hellman Key Exchange

Hashing Algorithms

a) MD5- (Message-Digest algorithm 5)

Cryptography can be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and secure data storage.

5. Secure Multi-Party Computation Protocol Using Asymmetric Encryption

Now a days people are interested to work with a third party rather than maintaining their own resources, in this circumstance there is a requirement of insuring security from the service provider as it may lead to security breaches and party may not be interested in such service providers. The solution incorporates protocol using asymmetric encryption scheme where any party can encrypt a message with the public key but decryption can be done by only the possessor of the decryption key (private key). As the protocol works on asymmetric encryption it ensures following

1. Confidentiality (Anonymity)
2. Security
3. Privacy (Data)

Secure Multi-Party Computation (SMPC) is needed to perform a joint computation over private data. Using SMC two parties can generate a random number R = AcB such that prime no's A, B cannot be obtained by individual party but it can be recovered jointly if needed.

6. Secure Cloud Computing Algorithm Using Homomorphic Encryption and Multi-Party Computation

The Homomorphic Encryption (HE) is performed on the encrypted data without decrypting it in computationally powerful clouds and the Secure Multi-Party Computation (SMPC) can be used in the cloud to ensure security and privacy of the users. A party is able to jointly perform computations without revealing their data to the other party. After combining Homomorphic encryption and Multi Party Computation (HE +MPC), the confidentiality and integrity of the data is maintained and the overhead is less than Homomorphic Encryption but more than Multi Party Computation. The Proposed Algorithm is based along the four phases: Key Generation, Encryption, Homomorphic Encryption (HE) and Multi Party Computation (MPC), and Deception. The main goal is to minimize the running time, cost, and the overhead during these four phases [1].

3. Proposed Technology

Homomorphic Encryption

Homomorphic encryption allows different ways of mathematical computation which is to be performed on the encrypted data without negotiating the encryption and letting the users data to be private. It transforms one data set into another form of data set and also preserves the relationship between both the data set. The term homomorphic is derived from Greek words “same structure” because the encryption scheme retains the same structure and operations whether they are performed on decrypted or encrypted data they will give the same results. Homomorphic encryption assumes a critical job in organizations so as to store the information on open cloud and furthermore takes the benefits of the administrations given by the cloud. A simple example of how a homomorphic encryption might work in cloud computing is given as:

Let us consider there is a company A which contains data set that has three numbers 20, 10 and 50.

Now the company A wants to perform some computation on the data, so it first encrypts the data in its own encryption technique. Suppose company decide to encrypt the data by multiplying all the numbers by 3 so the new numbers will become 60, 30 and 150.

The next step is storing the data set on the cloud for safe storage. A few days later another business contacts business A and requests for the sum of data set.

Since business A is busy, it contact cloud to perform the operation. The cloud performs the computation and returns the value 240 (60+30+150).

Final step is decryption which is done by business A and the decrypted answer received is 80.

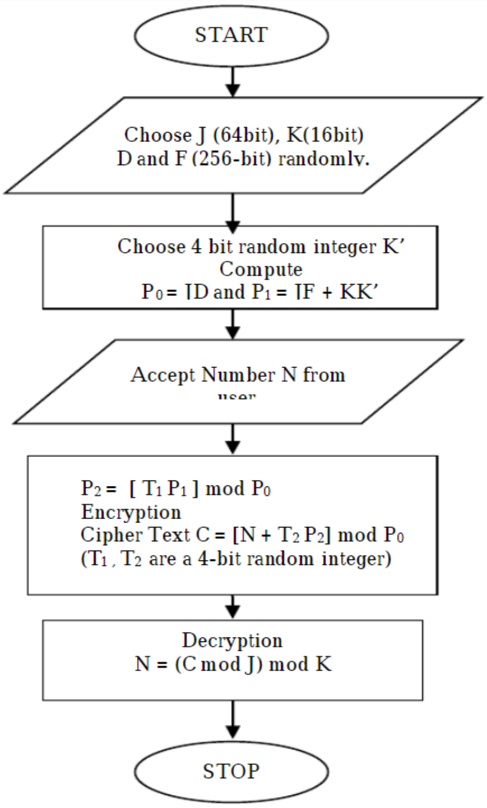
Amazon Web Services

Amazon Web Services (AWS) began to offer IT administrations to the market as web administrations, which is presently a days known as distributed computing. With this cloud, we need not anticipate servers and other IT foundation which requires up a lot of investment ahead of time. Rather, these administrations can in a split second turn up hundreds or thousands of servers in minutes and convey results quicker. We pay just for what we use with no straightforward costs and no long haul responsibilities, which makes AWS cost effective.

Today, AWS gives a very dependable, adaptable, ease foundation stage in the cloud that powers huge number of organizations in 190 nations around the globe. Amazon Web Services was formally re-propelled on March 14, 2006 joining the three beginning administration contributions of Amazon S3 distributed storage, SQS, and EC2.The project uses AWS services for multi-party computation where different users can store their private data on the cloud in the encrypted form. Once the data is stored any party can perform the different computation such as addition, subtraction, multiplication and some of the other functions like sum, maximum and minimum on their private data. In this way the integrity of the data is secured and computation is perform.

4. Implementation

In this project we have use the fully homomorphic algorithm to perform different operations like addition, subtraction and multiplication. Some of the other aggregate functions are also performed like Sum, Maximum and Minimum. The user can store their data on the cloud which can be a single number or an array of numbers. When any user wants to perform computation on their data then they can simply perform it with the help of following algorithm. The homomorphic algorithm uses different keys and the scheme is simplified and efficient version applied in AWS public cloud for security of users data. (J, K) represent a secret Key and (P0, P1) forms a public key. Number N to be encrypted is accepted as user input. The flowchart shows the proposed scheme to perform fully homomorphic algorithm.


START
Choose J (64bit), K(16bit)
D and F (256-bit) randomly.
Choose 4 bit random integer K'
Compute
P0 = JD and P1 = JF + KK'
Accept Number N from user
P2 = [T1 P1] mod P0
Encryption
Cipher Text C = [N + T2 P2] mod P0
(T1 , T2 are a 4-bit random integer)
Decryption
N = (C mod J) mod K
STOP

For Example:
Information is given as J=14883982794894487223, K=43321 and number to be encoded N=9
At that point D and F are determined as
D=70677186543966147614195862042065680704217811307170938823680817972460078770747 and
F=73039047329961611877474622320644292204439326844747783070676806904287578243639
Consider four piece number K' = 12 at that point register
P0=1051958028511940305929320607565533427835574146640991376691781227504638919782237324865124737665581
P1=1087111923814632766481581241697004087337750199678917794234945876512572829144575038603913867044349
Perform Encryption and get
C=351538953026924605522606341314706595021760530379264175431646490079339093623377137387891293787689.
Decryption is performed and get back plain content N=9

5. Conclusion

In this paper, we proposed a secure cloud computing model in which efficient cryptographic technique Based on Homomorphic Encryption (HE) And Multi-party Computation (MPC) was used to encrypt user's data followed by operations on their data while maintaining integrity and confidentiality. A party is able to jointly perform computations without revealing their data to the other party.

6. Future Work

A numerous research can be performed in this filed. We can use secure multiparty computation in numerous places in order to provide security of the private data in cloud.

The following are some modifications or possible up gradation that can be pursued in the future:

1. Division operation
2. Average operation

7. References

1. Das D. Secure cloud computing algorithm using homomorphic encryption and multi-party computation, in 2018 International Conference on Information Networking (ICOIN), 2018, 391-396.
2. Shukla S, Sadashivappa G. Secure multi-party computation protocol using asymmet-ric encryption, in International Conference on Computing for Sustainable Global Development (India. Com), 2014, 780-785.
3. Rishav Chatterjee, Sharmistha Roy. Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud in International Journal of Engineering Science and Computing, 2017.
4. Prakash C, Dasgupta S. Cloud computing security analysis: Challenges and possible solutions, in International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, 54-57.
5. Song X, Wang Y. Homomorphic cloud computing scheme based on hybrid homo-morphic encryption, in 2017 3rd IEEE International Conference on Computer and Com-munications (ICCC), 2017, 2450-2453.
6. Gouri Ajeev, Karthik Karunakaran, Arpita Gaur, Priya G. Review on Security Management in Cloud computing., in (2017). International Journal of Engineering and Computer Science I. 2016.
7. Shabnam Kumari PSK, Reema. In Security in Cloud Computing using AES DES, April International Journal on Recent and Innovation Trends in Computing and Communication, 2017.
8. Manish Potey M, Dr. Dhote CA, Deepak Sharma H. On Homomorphic Encryption for Security of Cloud Data, 2016.