Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

AN APPROACH ON SECURITY AND EFFICIENT CLOUD COMPUTING ALGORITHM USING FULLY HOMOMORPHIC AND SHELTERED MULTI PARTY COMPUTATION

[1]Shaikha Barkha, [2]Dr. S. Sathish Kumar
[1]PG Scholar, MTech, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.
[2]Professor, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.

Abstract- To legion safety issues the distributive computing is creating innovation. Content of the untrusted mists could be jumbled by means of encipher calculation. Randomizing content gives greater security that could be accomplished by padding concept inside the cloud. In this material, the client's content is scrambled by padding plan, referred as Optimal Asymmetric Encryption Padding (OAEP) with Hybrid Encryption computing that is firmly based on RSA (i.e., HE-RSA), so it enables multiple gatherings to process a capacity on their raw data sources while insulating reliability and Confidentiality. The Homomorphy Encryption (HE) is improvised on the jumbled content free from decoding; Secure Multi-Party Computing (SMPC) is applied in the cloud to provide safety to the clients. Under the material, this proposed plan incorporates the multi-party computing with homomorphy encryption to permit figuring's of encoded content not with unscrambling. The cryptographic strategies applied in cloud are depicted and overheads are contrasted and Homomorphy Encryption and Multi-Party Computing.

KEYWORDS
Cloud Computing; Optimal Asymmetric Encryption Padding; Homomorphic Encryption; Multiparty Computation.

I. INTRODUCTION

There is a requirement for a proper or increasingly appropriate enormous information framework that bolsters the capacity and preparing on a high scale. Presently a days the world is information driven, hence the huge information handling and investigation have turned into the most significant errand for any vast foundation. The distributed computing is a model to give helpful, on-request access to share the figuring assets. Associations can essentially interface with the cloud and utilize the accessible assets on the best possible utilization premise. The distributed computing has turned into an apparatus for dissecting enormous information utilizing shared processing assets while effectively dealing with changes in the volume and assortment of the information. The cloud gives numerous focal points, for example, more adaptation to non-critical failure and multi-factor authentication to secure the data in the cloud. In any case, the distributed computing additionally accompanies hazards in keeping up the confidentiality and trustworthiness of information because of these properties. Over the most recent couple of years, there have been expanding the quantity of information breaches in the cloud because of malignant and meddlesome activities. Encryption keeps the information very still secure however information is lost in the event that we lose the encryption key. Consequently, to counteract the vindictive assaults on the cloud, it is important to create proficient cryptographic procedures which is impervious to dynamic assaults just as performing computations of encoded information without unscrambling. The distributed computing based arrangements have turned out to be progressively prevalent in the previous couple of years. The distributed computing stage breaks down and separates valuable data from the Big information cloud. One of the primary worries with distributed computing has been the protection and confidentiality of the information in the cloud. One arrangement is to send the information scrambled to the cloud. In any case, despite everything we have to help valuable computations on the encoded information and Fully Homomorphic Encryption (FHE) is a method for supporting such computations on scrambled information. We note that while other systems exist for secure computation, they by and large require the various information suppliers to trade data. Since FHE schemes are open key schemes, FHE is greatly improved appropriate for the situation where we have numerous wellsprings of information.

The Secure Multi-Party Computation (MPC) ensures that everybody learns the right yield of a joint computation yet nothing else about any other individual's data sources, notwithstanding when a portion of the client playing out the computation may be effectively or latently noxious. Secure MPC should be possible for self-assertive computations and for any number of gatherings. Hence, we can see secure MPC conventions as compilers that take as info a detail of a capacity and yield a convention that registers the capacity securely. Hence, we can see secure MPC conventions as compilers that require as information a determination of a mapping and yield is a convention that registers the capacity securely. The Secure MPC offers the two confidentialities just as uprightness which is vastly improved than fully homomorphic encryption and undeniable computation. Trustworthy MPC can be performed for subjective computations and for any number of parties in Cloud Environment.

The benefits of our model:

- Integrates multi-party computation with homomorphic encryption
- Proposes a plan to use Optimal Asymmetric Encryption Padding(OAEP)-Homomorphic Encryption(HE)-RSA for encryption.

II. RELATED WORK

M. Tebba et al. proposed a technique to execute operations on encrypted data in the cloud which will provide us with the similar results after calculations as though we have worked directly on the crude data. Z. Wang et al. gave a fresh definition of homomorphic signature for identity management in mobile cloud computing. S. Yakoubov et al. conducted a survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud. C. Rong et al. conducted a survey on different security challenges in Cloud Computing. C. Gentry computed arbitrary functions of encrypted data which describes a fully homomorphic encryption technique that keeps information private, however that leaves a worker that does not possess the private decryption key to compute any result of the data, even when the purpose of the data is really complex. C. Wang et al. proposed an effective scheme with two salient features to ensure the correctness of the user's data in the cloud. Y. Yu et al. investigated the active adversary attack in three auditing mechanisms for shared data in the cloud and also proposed a solution to remedy the weakness without sacrificing any desirable features of these mechanisms. L. Wei et al. proposed a privacy cheating discouragement and secure computation auditing protocol, or SecCloud, which is a first protocol bridging secure storage and secure computation auditing in cloud. A. Lopez-Alt et al. showed a new type of encryption scheme which they called multi key FHE. F. F. Moghaddam et al. proposed a hybrid encryption algorithm based on RSA Small-e and Efficient-RSA for cloud computing environments. E. Shen et al. proposed a scheme which is called Cryptographically Secure Computation in the cloud utilizing the concept of secure multi-party computation. This is a cryptographic approach that enables information sharing and analysis while keeping sensitive sources of info secret faster and easier to use for application software developers. M. Bellare et al. proposed Optimal Asymmetric Encryption with RSA. This work aimed to use the cryptography concepts in cloud computing communications and to increase the security.

D. Zissis et al. addressed the details of cloud computing security issues and they proposed Public Key Infrastructure operating based on SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, inside which essential trust is maintained. C. Hongbing et al. presented an alternative approach called secure Big Data Storage and Sharing Scheme for Cloud Environment. Tenants which divides huge data into sequenced parts and stores them among multiple Cloud storage service providers. Instead of protecting the huge data itself, the proposed scheme protects the mapping of the different data elements to each provider utilizing a trapdoor function. The cloud computing reviewed was presented in the paper. In this paper creators have discussed the relationship between enormous data and cloud computing, huge data storage systems, and Hadoop technology. Furthermore, research challenges are investigated, with focus on scalability, availability, data integrity, data transformation, data quality, data heterogeneity, privacy, legal and regulatory issues, and governance. Lastly, open research issues that require substantial research efforts are summarized.

J. Zhou et al. proposed a scheme called Secure and Privacy Preserving Protocol for Cloud-based Vehicular DTNs which solved the open problem of resisting layer-adding attack by outsourcing the privacy-preserving aggregated transmission evidence generation for multiple resource constrained vehicles to the cloud side from performing any one-way trapdoor function only once. The vehicle privacy is well protected from both the cloud and transportation manager.

III. PROBLEM FORMULATION FOR SECURE CLOUD COMPUTING

Consider three parties (appeared in Fig. 1): a user Alice that stores her data in the cloud; a user Bob with whom Alice needs to share data; and a cloud service provider that stores Alice's data. To use the service, Alice and Bob begin by downloading a client application that consists of a data processor, a data verifier and a token generator. Upon its first execution, Alice's application generates a cryptographic key. We will refer to this key as a master key and assume it is stored locally on Alice's system and that it is kept secret from the cloud service provider. Cloud security is measured in terms of Availability, Integrity, and Confidentiality and encryption techniques are prone to a number of attacks like:

Availability:

In this scenario cloud service providers have multiple servers. When one server fails, there is no security issue as another server is ready to provide services

Integrity:
The data integrity means the correctness and trustworthiness of the data. It ensures that the computation on sensitive data is correct. The data cannot be altered by the unauthorized user.

Confidentiality:
Confidentiality is to prevent sensitive information from the reach of the attacker, while making sure that the authorized user have access to it. Services require user to confide in the cloud with their data. However, in the untrusted cloud Data owners do not confide in the cloud. Along these lines user side protection is necessary. Users encrypt their data before putting away into the cloud with the help of a public key.

Fig. 1. *Cloud Architecture under various Cryptographic Techniques*

Cycle attack:
In this attack, the cipher text is encrypted repeatedly and the no of iterations are counted until the original text appears. It can decrypt any cipher text.

Cipher text attack:
In this attack, both the plaintext and the cipher text is known to the attacker and he can use this to discover private exponent and once it discovered it is easy to find then. Multiple parties wish to perform operations on their sources of info. This requires decryption of their data. This poses security problems on account of untrusted Clouds.

Can multiple parties store their data with efficient cryptographic techniques that are resistant to attacks and perform the computations without decrypting their data?

IV OBJECTIVE

The Cloud environment requires protection and confidentiality of user data while leveraging computation ability of entities in the cloud network directly on encrypted data. This paper focuses on an issue that is attractive to many types of research, which is a data encryption for cloud computing. Cloud environment requires security and confidentiality of user data while leveraging the computational ability of entities in the cloud network directly on encrypted data. In this paper, we have proposed a scheme that integrates the multi-party computation with homomorphic encryption to allow calculations of encrypted data without decryption.

OUR CONTRIBUTION

In our paper, we have proposed an efficient cryptographic technique by padding the multiple party data before encrypting it. The user's data is encrypted utilizing padding scheme Optimal Asymmetric Encryption Padding (OAEP) together with Hybrid Encryption algorithm that is based on RSA Small-e and Efficient RSA (HE-RSA). So as to allow multiple parties to compute a function on their sources of info while preserving Integrity and Confidentiality. The homomorphic encryption is performed on the encrypted data without decrypting it in computationally powerful clouds. The proposed scheme integrates the multi-party computation with homomorphic encryption to allow calculations of encrypted data without decryption. The yield of this nature allows maintaining confidentiality and integrity in the cloud environment.

IV. CRYPTOGRAPHIC TECHNIQUE FOR SECURE CLOUD COMPUTING

To interact with various services in the cloud and to store the data generated/processed by those services, several security capabilities are required. In order to achieve this we have six modules in our project, Which are listed below:

- **User Interface Design**
- **Users**
- **Encryption**
- **Decryption**
- **Secure Multi-Party Computation (SMPC)**
- **Admin**

DESCRIPTION

- **User Interface Design**

In this module we design the page for the project. These pages are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

- **Users**

Users Register & enter name & password Login into application. After that Upload files when our Uploading encrypt data & server will generated by each and every file one different key. If any user sent file key request given response & sending particular file key. Communicating integrates the multi-party computation user's.

JES
Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

➢ **Encryption**

In this project, the user's data is encrypted using padding scheme, called Optimal Asymmetric Encryption Padding (OAEP) together with Hybrid Encryption algorithm that is based on RSA (i.e., HE-RSA), in order to allow multiple parties to compute a function on their inputs while preserving Integrity and Confidentiality. All files are stored in different tables based on file capacity and encrypt the file, which are stored in Cloud storage.

➢ **Decryption**

Users Register & Login into application. After that Upload files.

When our Uploading encrypt data & server will generated by each and every file one different key.

1) If user sent file key request.
2) File owner if accept the request given response & sending particular file key.
3) Enter File key Decrypt data & Download files.

ALGORITHM

Algorithm 1 Algorithm for Secure Cloud Computing

Step 1: Key generation algorithm: keygen(p,q)
Randomly choose two large primes p ,q and compute n=p.q
.
$\phi(n) = (p-1)(q-1)$
$\Upsilon(n,h) = (p^h - p^0)(p^h - p^1) \ldots\ldots\ldots\ldots\ldots (p^h - p^{h-1})(q^h - q^0)(q^h - q^1) \ldots\ldots\ldots (q^h - q^{h-1})$
Select random integer r such that $1 < r < n$ and $gcd(R, \Phi) = 1$ and $gcd(R, \Upsilon) = 1$
Compute e such that $r.e = 1 \bmod \Phi, 1 < e < \Phi(n)$
Compute d such that $d.e = 1 \bmod \Upsilon, 1 < d < \Upsilon(n)$
Public key(pk): (e,n)
Secret key(sk): (r,d,n)
Step 2: : Encryption: Enc(M,pk)
Suppose Sender and Receiver send data to M1 and M2 respectively to the cloud
$G : \{0,1\}^{K0} \longrightarrow \{0,1\}^{K0}$
$H : \{0,1\}^{K-K0} \longrightarrow \{0,1\}^{K-K0}$
$r \longleftarrow \{0,1\}^{K0}$
$S = (M \parallel 0^{K1}) \oplus G(r)$
$t = r \oplus H(s)$
$C \longleftarrow \ll S \gg^e \bmod n \gg^e \bmod n$
Return C
Step 3: Homomorphism and Multi-party computation
Homomorphic computations are performed on Sender and Receiver encrypted data C1 and C2 respectively.
$C1 = ((M1)^e \bmod n)^e \bmod n$
$C2 = ((M2)^e \bmod n)^e \bmod n$
$C1.C2 = [((M1)^e \bmod n)^e \bmod n][((M2)^e mod$ n$)^e \bmod n]$
$= ((M1)^e \bmod n)^e((M2)^e \bmod n)^e \bmod n$
$= ((M1M2)^e \bmod n)^e \bmod n$
$LetC = C1.C2, M = M1M2$
$C = (M^e \bmod n)^e \bmod n$
Step 4: Decryption: Dec(C,sk)
Sender and Receiver decrypt the computed data C using their respective private keys
$W \longleftarrow (C^r \bmod n)^d \bmod n$
Parse W as $s \| t$
$r \longleftarrow H(s) \oplus t$
$M^1 \longleftarrow s \oplus G(r), parseM^1 asM \| Z$

➢ **Secure Multi-Party Computation (SMPC)**

The proposed secure cloud computing algorithm is ensuring the security and privacy of individual data in the cloud along with the enhancement of the security mechanism like Homomorphic Encryption and Multi Party Computation (MPC). The Proposed Algorithm is based along the four phases: Key Generation, Encryption, Homomorphic Encryption (HE) and Multi Party Computation (MPC), and Deception.

➢ **Admin**

In this module only single admin is there first enter admin name & password login to server this is the authentication process of our project. After login if you want search any files like .txt, .docx, .pdf, .jpg files. After that view all upload files details. If you want move the data one table to another table it will send

SYSTEM ARCHITECTURE

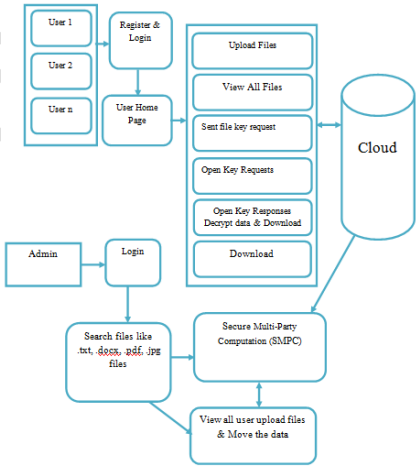

Fig 2: system architecture

V. RESULTS

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. So, we have received moderate overhead based on the Homomorphic Encryption and Multi Party.

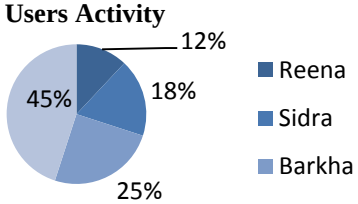

Fig 3: User Activity Representation

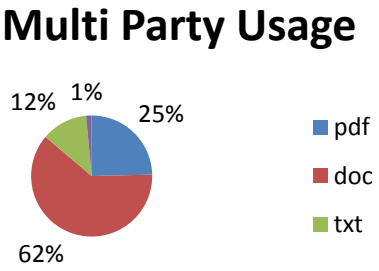

Fig 4:Multiple Party Usage Representation

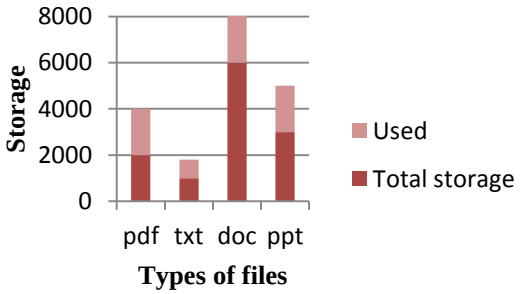

Fig 5 :Storage and availability

VI. 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. The yield is same as though the operations have been carried on crude data. A party can jointly perform computations without revealing their data to the other party. Here, we designed and developed secure homomorphic encryption and multi-party computation techniques tailored specifically for a private semi-trusted cloud setting. This setting allows developers to design the private cloud together with the cryptographic techniques (i.e., HE+MPC) necessary to protect it.

REFERENCES

[1] Mell P, Grace T. The NIST definition of cloud computing, NIST Special Publication, 2009, pp. 800–145.

[2] Tebaa M, Hajji S.E, Ghazi A.E. Homomorphic Encryption Applied to the Cloud Computing Security, Proceedings of the World Congress on Engineering, London, U.K., Vol.1, No.1, 2014, pp. 4-6.

[3] Wang Z, Sun G, Chen D. A new definition of homomorphic signature for identity management in mobile cloud computing, Journal of Computer and System Sciences, Vol. 80, N0. 3, 2014, pp. 546-553.

[4] Yakoubov S, Gadepally V, Schear N, Shen E, Yerukhimovich A. A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud, IEEE High Performance Extreme Computing Conference (HPEC), 2014, pp. 1–6.

[5] Rong C, Nguyen ST, Jaatun MG. Beyond lightning: A survey on security challenges in cloud computing, Computers and Electrical Engineering, Vol. 39, No. 1, 2013, pp. 47-54.

[6] Gentry C. Computing Arbitrary Functions of Encrypted Data, Communications of the ACM, Vol. 53, No. 3, 2010, pp. 97-105.

[7] Wang C, Wang Q, Ren K, Lou W. Ensuring Data Storage Security in Cloud Computing, Quality of Service, 2009, pp. 1–9.

[8] Yu Y, Niua L, Yang, G, Mu Y, Susilo W. On the security of auditing mechanisms for secure cloud storage, Future Generation Computer Systems, Vol. 30, 2014 pp. 127-132.

[9] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing, Information Sciences, Vol. 258, 2014, pp. 371-386.

[10] Lopez-Alt A, Tromer V, Vaikuntanathan E. On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption, Proceedings of the forty-fourth annual ACM symposium on Theory of computing, 2012, pp. 1219–1234.

[11] Brakerski Z,and Vaikuntanathan E. Efficient fully homomorphic encryption from (standard) LWE, SIAM Journal on Computing, Vol.43, No.2, 2011, pp. 831–871.

[12] Bellare M, and Rogawayy P. Optimal Asymmetric Encryption How to Encrypt with RSA, Advances in Cryptology Eurocrypt 94 Proceedings, Vol. 950, 1995, pp. 1–19.

[13] Shen E, Varia M, Cunningham RK, Vesey WK. Cryptographically Secure Computation, IEEE Computer Society, Vol. 48, No.4, 2015, pp. 78–81.

[14] Zissis D, Lekkas D. Addressing cloud computing security issues, Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583–592.

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

AUTHOR'S PROFILE

Ms. SHAIKHA BARKHA has completed her Shadan college of engineering and technology, Khairtabad, JNTU University Hyderabad. Presently, she is pursuing Masters in Computer science engineering from Shadan college of Engineering and technology, Hyderabad, TS. India.

DR. S. SATHISH KUMAR has completed B.E - Computer Science and Engineering from KSR College of Engineering, Tiruchengodu, Affiliated to Anna University, Chennai. M.E – Computer Science and Engineering from Sri Krishna Engineering College, Chennai, Affiliated to Anna University, Chennai. PhD from Annamalai University, Chidambaram. Currently working in Shadan Women's College of Engineering and Technology, Khairatabad as Associate Professor in Department of Computer Science and Engineering. He is having 5 years of experience in teaching and research.