ISSN: 2581-9674
Article ID: IJDCSE09202006
International Journal for Development of Computer Science and Engineering (IJDCSE)
Volume-2, Issue-5, September-2020, PP.40-49
www.ijdcse.org
Received: 03-07-2020, Accepted: 07-08-2020, Published: 08-09-2020 .

A STUDY ON HOMOMORPHIC ENCRYPTION METHODS FOR DATA SECURE

Er.SHIVA KUMAR
Bangalore

ABSTRACT

Cloud computing is an emerging technology in which large number of remote servers are linked together to allow sharing of information-processing tasks, centralized storage in database, and online access to computer resources and services. It helps people to improve their business by quickly improving service delivery capabilities without the need to spend money on acquiring new infrastructure, licensing software, and training for staff. A major hurdle to the adoption of cloud-based services is security related issues. Cloud users will be placing their sensitive information on cloud servers. Information may be encrypted and kept within the cloud however the matter is that whereas information may be sent to and from a cloud provider's information center in an encrypted type, the servers that power a cloud can't do any work on that manner. With homomorphic coding, an organization might cipher its entire information and transfer it to a cloud and it's attainable to research information while not decrypting it. In this paper, a study is made on homomorphic cryptosystems, their types disagree, the way to use them to secure our information in cloud and perform operations on the info with the assistance of cipher texts.

INTRODUCTION

Cloud computing is an emerging technology in which large number of remote servers are linked together to allow sharing of information-processing tasks, centralized storage in database, and online access to computer resources and services. It helps people to improve their business by quickly improving service delivery capabilities without the need to spend money on acquiring new infrastructure, licensing software, and training for staff. A major hurdle to the adoption of cloud-based services is security. Cloud users, notably at the enterprise and government level, are involved with losing management of, or simply plain losing, their information once it's placed within the cloud. The in corporeality of cloud storage makes it tough for customers to feel snug that their information is well protected by cloud service suppliers. Coding might alleviate this issue. However, if you wish to control your encrypted information within the cloud, the key to decipher your information should be shared with the cloud supplier. This avoids the concept of

using a secret key. Sharing this key in fact would enable this cloud supplier (or future supplier if the service changes hands) access to your information. The solution to the current downside might be homomorphic coding.

Cloud computing may be a new technique advises from the trade circle. It encompasses parallel computing, distributed computing and grid computing. It's a mix and evolution of virtualization of network, utility computing, Infrastructure-as-a-service-IaaS, Platform-as-a-Service-PaaS and Software-as-a-Service-SaaS. Cloud computing will give 3 varieties of service modes. SaaS refers to the services provided to purchasers, the applications working on cloud computing infrastructure provided by the service suppliers. PaaS refers to deploying the applications created by the event language and gear provided by the service suppliers to the cloud infrastructure. IaaS refers to the services provided to the users, to lease the process power, storage network and alternative basic computing resources. Four of these services, there's no want for users to manage or management the cloud infrastructure, as well as network, server, OS, storage and even the functions of applications.

Cloud computing is a web based mostly development and use of engineering and computing design within which information centers are reworked into pools of computing services by powerful processors beside SaaS design. Cloud computing may be a results of usage of technology for day to day activities through net Cloud computing came into the foreground as there have been advances in virtualization, distributed computing with server clusters and increase within the handiness of broadband net access. IT trade describes cloud computing merely because the delivery of applications provided by a 3rd party over the web.

SECURITY THREATS IN CLOUD

According to Cloud Security Alliance-CSA [1] there are few most rife and high security threats in cloud computing. Few of them are explained in short below.

1. Information Breaches

The data breach at Target, leading to the loss of private and credit card info of up to a hundred and ten million people.

2. Data Loss

A data breach is that the results of a malicious and possibly intrusive action. Information loss could occur once a drive dies while not its owner is having created a backup. It happens once the owner of encrypted information loses the key that unlocks it.

3. Account Or Service Traffic Hijacking

Account hijacking sounds too elementary to be a priority within the cloud; however CSA says it's a drag. Phishing, exploitation of package vulnerabilities like buffer overflow attacks, and loss of passwords and credentials will all cause the loss of management over a user account. A trespasser with management over a user account will listen in on transactions, manipulate information, give false and business-damaging responses to customers, and direct customers to a competitor's website or inappropriate sites.

4. Malicious Insiders

Malicious insiders might sound to be a standard threat. If one exists within an oversized cloud organization, the hazards are exaggerated. One maneuver cloud customers ought to use to safeguard them is to stay their coding keys on their own premises, not within the cloud network.

5. Abuse Of Cloud Services

Cloud computing provides large-scale, elastic services to enterprise users and hackers similarly. "It may take assailant years to crack a coding key utilizing one's own restricted hardware. However utilizing an array of cloud servers, he could be able to crack it in minutes," the report noted. Or hackers may utilize cloud servers to spread malware, launch attacks like DDoS, or distribute pirated package.

In this paper the focus is mainly on data breach security threat which can be handled using a robust Encryption technique.

PREVIOUS WORK

There are several works done earlier to unravel the info breach security threat. Many are mentioned below.

A method was proposed by Dimakis et al. [2] for increasing the probability of avoiding data breach. They thought-about the case that n= ak for a set constant a. it's shown that distributing every block of a message to 'v' chosen random storage servers is enough to have a likelihood/probability *1-k/p-o(1)* of prospering information retrieval ,where v=b ln k, b>5a and p is that the order of used cluster. The meagerness parameter v = b ln k is that the range of storage servers that a block is shipped to. The larger v is, the communication price is higher and therefore the prospering retrieval likelihood is higher. The system contains little confidentiality as a result of an assailant will compromise k storage servers to urge the message.

The confidentiality and robustness problems in cloud computing was addressed by Lin and Tzeng [3] by providing a secure suburbanized erasure code for the networked storage system. Additionally to storage servers, their system consists of key servers that hold cryptographical key shares and add a distributed manner. In their system, keep messages are encrypted and encoded. To retrieve a message, key servers question storage servers for the user. As long because the

range of accessible key servers is over a threshold t, the message may be with success retrieved with an amazing likelihood. Their results shows that once there are n storage servers with n= ak√k, the parameter v is b√k ln k with b>5a and every key server queries a pair of storage servers for every retrieval request, the likelihood of a prospering retrieval is a minimum of 1-k/p-o[1].

Hsiao-Ying Lin and Wen-Guey Tzeng [4] developed an extremely distributed system with parameters $n=a\ kc$ where c≥1.5 and a> √2. The system supports secure information/data forwarding by utilizing threshold proxy re-encryption theme. Here the quantity of storage servers is far bigger than the quantity of blocks of a message.

Two proxy re-encryption methods were suggested in [5, 6]. In an exceedingly proxy re-encryption theme, a proxy server will transfer a cipher text underneath a public key PK_A to a brand new one underneath another public key PK_B by utilizing the re-encryption key RK_{A-B}. The server doesn't recognize the plain text throughout transformation.

A system was proposed by Ateniese et al. [7] within which messages are 1st encrypted by the owner and so keep in an exceedingly storage server. Once a user desires to forward his messages, he sends a re-encryption secret key to the web storage server. The storage server re-encrypts the encrypted messages for the licensed user.

A homomorphic coding theme was proposed by Mahadevan Gomathikrishnan et al. [8] utilizing Residue Number System [RNS]. Here a program P is rib into k threads. All the key variables which have to be protected are separated into k moduli utilizing RNS. Every thread would have identical management flow completely different information. During this theme a secret data is split into multiple shares on that computation may be performed severally. Security is increased by not permitting independent clouds to interact. Potency is achieved through the smaller shares.

Emalda roslin et al. [9] projected a technique within which a cloud server splits into completely different chunks and so encrypted. Then the encrypted cloud server is unbroken in an exceedingly duplicate cloud server as a backup. The encrypted information is converted back to bytes and so more with check bit by the information owner so as to limit the TPA by accessing the first data.

Osama Khan et al. [10] projected an algorithmic program that finds the best range of code word symbols required for recovery for any XOR based mostly erasure code and produces recovery computer hardware that use a minimum quantity of information.

Aderemi and Oluwaseyi [11] projected a searchable parallel coding theme which allows a user to by selection search the info that the user hosted within the cloud. An encryption layer above the encrypted files to keep within the cloud network. This further layer would be an encrypted search index layer which might be searched unitizing secure indexes.

Cloud computing security is an emerging sub-domain of computer system security, network security and additional generally data security.

HOMOMORPHIC ENCRYPTION ALGORITHM

Homomorphic is that the ability to execute computations on the cipher text while not decrypting it 1st. Our final goal is to use a completely homomorphic coding theme E. Fully homomorphic method is explained below.

At a high-level, the essence of fully homomorphic coding is simple: given cipher texts that encrypt m1, m2, m3,……mt, fully homomorphic coding ought to enable anyone (not simply the keyholder)

To output a cipher text that encrypts f(m1,m2,m3,……mi) for any desired function f(m), as long as that operate is with efficiency computed. No info concerning m1, m2, m3,……mt or f(m1,m2,m3,……mt) or any intermediate plaintext values, ought to leak; the inputs, output and intermediate values are forever encrypted.

Formally, there are alternative ways of process what it suggests that for the ultimate cipher text to encrypt f (m1, m2,……mi). The minimal demand is correctness. A completely homomorphic coding scheme E ought to have an economical algorithmic rule Evaluate E that, for any valid E key pair (sk; pk), any circuit C, and any cipher texts

Ψi ← Encrypt E (pk; mi) outputs

Ψ← Evaluate E (pk; C; Ψ1 Ψ2…….. Ψt) such that

Decrypt E (sk;Ψ) = C(m1,m2,……mt).

If all data hold on within the cloud were encrypted, that might effectively solve problems like availableness, Data Security, and Third-Party management. However, a user might not be able to leverage the ability of the cloud to carry out computation on knowledge while not 1st decrypting it, or shipping it entirely back to the user for computation. The cloud supplier therefore must decipher the information 1st (nullifying the problem of privacy and confidentiality), perform the computation then send the result to the user. What if the user may do any discretional computation on the hosted knowledge while not the cloud supplier learning concerning the user's knowledge - computation is finished on encrypted data while not previous cryptography. This

can be the promise of homomorphic coding schemes which permit the transformation of cipher texts C (m) of message m, to cipher texts C (f(m)) of a computation/function of message m, while not revealing the message.

Rivest, Adleman and Dertouzos in 1978, suggested the idea of using RSA encryption for first time. RSA (invented by Rivest, Shamir and Adleman 78) [12] had increasing homomorphism (you may cipher a cipher text that is that the product of plaintexts) and many other researchers came up with part homomorphic cryptosystems. A survey on homomorphic coding schemes is found in [13, 14].

A fully homomorphic encryption-FHE enables us to compute the encrypted data into the cloud without knowing the secret key.

FHE Algorithm Implementation in cloud computing

Fully homomorphic encryption Utilization assures data security for cloud computing. The key concept is that the information is encrypted by homomorphic coding and holds on in cloud server, through this we will get the massive benefit: cope with the cipher text directly in server and assure the data's security as a result of anyone else who doesn't apprehend the key can't decipher it. We tend to use symmetric homomorphic coding to construct the information secure theme.

The homomorphic symmetric cipher scheme:

Select encryption parameter: z, x and y, $z \sim 2^n$, $x \sim 2^{n2}$, $y \sim 2^{n5}$ and x is prime

X is that the secret key

Encrypt: for plain text 'm'

Compute $c=x*y+2z+m$ wherever c is that the cipher text

Decrypt: $m = ((c \bmod x) \bmod 2)$

Correctness: since xy is larger than 2z+m, $(c \bmod x) = 2z+m$

Finally $(c \bmod x) \bmod 2 = (2z+m) \bmod 2 = m$

Homomorphic: for 2 cipher text

$C_1 = y_1 x + 2y_1 + m_1$

$C_2 = y_2 x + 2y_2 + m_2$

Computation:

$C_1 + C_2 = (y_1+y_2) *x+2(z_1+z_2) +m_1+m_2$

So if $2(z_1+z_2) +m_1+m_2 << x$,

Then $(c_1+c_2) \bmod x=2(z_1+z_2) +m_1+m_2$

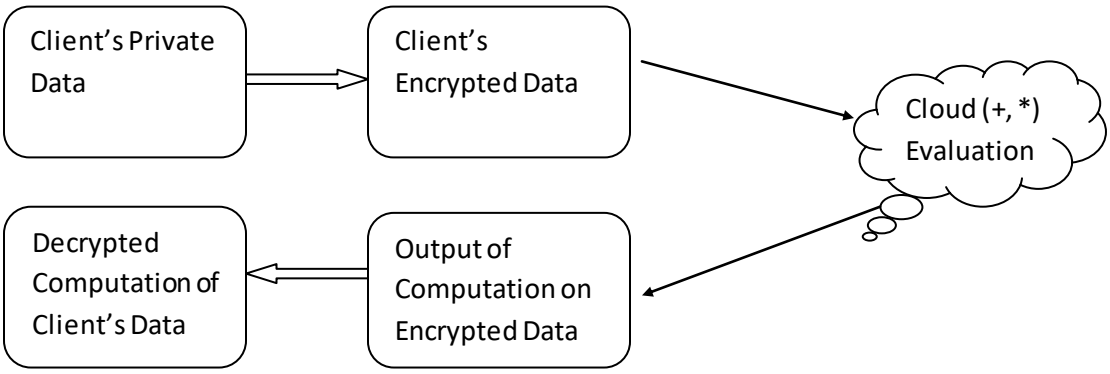
The above one is additive homomorphic.

And $c_1*c_2= [y_1*y_2x+ (2z_1+m_1) + (2z_2+m_2)] \; x+2(2z_1 \; z_2+z_1m_1+z_2 \; m_1) +m_1 \; m_2$

So if $2(2z_1 \; z_2+z_1m_1+z_2 \; m_1) +m_1 \; m_2 << x$
Then

$(c_1*c_2) \bmod x=2(2z_1 \; z_2+z_1m_1+z_2 \; m_1) +m_1 \; m_2$

Using this above FHE scheme, we can design secure cloud data scheme: It is shown in below figure.



As the figure shows it utilizes bilaterally symmetric homomorphic cipher to boost data security. The client will encrypt his plain texts using a secret key generated. Then the encrypted data will be stored on Cloud Storages. If an intruder tries to hack into storage then he will find only the encrypted data. Later the client can decrypt data when needed using the same key.

Additionally alternative cryptograph technology like digital signature can be applied to assure the integrity and non repudiation. At last, the user will send request to cloud server (also encrypted) and also the server do the operation even while not grasp the content of the operation. With this scheme, not solely the keep data however additionally the transmitted data is encrypted, therefore we tend to don't worry concerning the information is eavesdropped or purloined. It can also give secure knowledge audit service as a result of the third audit party can handle the encrypted knowledge directly. And also the secret writing we tend to use is symmetry therefore we are able to figure it with less million instructions per second that are vital for skinny consumer.

CONCLUSION

In this paper we've got analyzed the various security issues present in cloud computing. When consumer send info to the server in encrypted kind to perform any procedure operation thereto encrypted knowledge server would like the personal key from the consumer. If consumer offers that personal key then the privacy isn't ensured, once more the way to make sure that nobody can perform any unauthenticated operation with the information. During this paper we've got given some totally homomorphic secret writing theme developed by researchers which permit us to perform computation on encrypted knowledge while not exploitation secret key of consumer. It's nothing however a replacement layer applied to the cloud computation. A sensible FHE answer would see widespread use by cloud service suppliers, considerably hardening cloud security and creating cloud storage an additional viable choice for shoppers. Researchers worldwide are actively engaged in making an attempt to give a sensible fully homomorphic encryption solution.

REFERENCES

[1] The Cloud Security Alliance, worst cloud security threats http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085?page_number=2

[2] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Decentralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[3] H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage , ," IEEE Trans.Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[4] H.-Y. Lin and W.-G. Tzeng, "A Secure Erasure Code based cloud storage system with secure data forwarding," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, June. 2012.

[5] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54- 63, 1997.

[6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 127-144, 1998.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[8] Mahadevan Gomathikrishnan,Akilesh Tyagi," HORNS-A Homomorphic encryption scheme for cloud computing using Residue Number System", IEEE transactions on parallel and distributed systems, vol. 23, no. 6, June 2011,pp 995-1003.

[9] Emalda Roslin, Abhirami, Nandita,"SSS-ECSecure storage services and erasure code implementation in cloud computing ", IJETT, vol.4, no.3, June 2013,pp 275-283.

[10] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, "Rethinking erasure codes for cloud file systems: Minimizing i/o for recovery and degraded reads, FAST 2012.

[11] Aderemi A Atayeo,Oluwaseyi Feyistan,"Security Issues in Cloud Computing-The potentials of Homomorphic Encryption",JETCI,Vol 2,no 10,October 2011,pp546-552.

[12] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In Comm. of the ACM, 21:2, pages 120–126, 1978

[13] C. Fontaine , F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007,p.1-15, January 2007

[14] D. Micciancio and O. Regev. Post-Quantum Cryptography, chapter Lattice-based Cryptography. Springer, 2008