IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-6 E-ISSN: 2347-2693

# A Review of Homomorphic Encryption Algorithm for Achieving Security in Cloud: Review Article

**Abhishek Satyarthi[1*], Sanjiv Sharma[2]**

[1*]CSE/IT Dept., Madhav Institute of Technology and Science, RGPV, India
[2]CSE/IT Dept., Madhav Institute of Technology & Science, RGPV, Gwalior, India

**Corresponding Author: pchaturvedi1118@gmail.com, Mob.: +91-9406983296*

**Available online at: www.ijcseonline.org**

Received: 29/May/2017, Revised: 10/Jun/2017, Accepted: 24/Jun/2017, Published: 30/Jun/2017

***Abstract*—** Cloud computing has created a brief exchange in code paradigm and being extraordinarily new generation however has been followed extensive through numerous groups and character for his or her computing wants. Definition of Cloud Computing is definitely unique from definitions provided thru researchers. Cloud computing is emerging paradigm gives various IT associated offerings. The safety and privacy are maximum critical elements that inhibits the boom of cloud computing. Security factors are reasons behind lesser amount of actual instances and business enterprise associated cloud applications in assessment to consumer related cloud software program. “Cloud computing can be a model for permitting omnipresent, on hand, on-name for Network get admission to to a shared pool of configurable computing sources (e.g., networks, servers, storage, applications, and services) that may be rapid provisioned and discharged with tokenism manage strive or service organization interaction. This cloud model includes five critical traits, three service fashions (Software as a Service (SaaS). Platform as a Service (PaaS). Infrastructure as a Service (IaaS) and 4 education fashions (Private, Community, Public and Hybrid varieties of cloud)”. The developing pace of cloud is as a substitute brief.

***Keywords*—** Cloud Computing, homomorphic coding algorithmic rule, Security Challenges, Integrity

## I. INTRODUCTION

Security is major concern to the cloud computing. There's sturdy thrust to produce security at infrastructure network level, Host level, application level and information. The information is related to every level like network, host and Application level. During this paper security of cloud information at rest is concentrated. Cloud computing uses many technologies [1]. The safety problems associated with completely different sort attacks associated with many technologies has to be addressed. Some security problems in cloud computing includes:

• **Accessibility** –Availability of knowledge is a very important security issue. Whenever it's needed it should create accessible to user. Additionally user should have management over its information. Accessibility issue has to attend, once service is needed from another cloud service supplier. There square measure presently 3 major threats to accessibility. The primary threat is network primarily based attack 2. The second threat is cloud service suppliers accessibility and third backup of keep information by cloud service supplier. There’s got to give effective and economical techniques for access management, authentication and authorization of great information.

• **Information Remanence** - it's a problem once information gets exposed when deletion to the unauthorized party. an information security lifecycle refers to the complete method from information creation to destruction is shown in Fig. 1. Care should be taken once the information has to be destroyed.

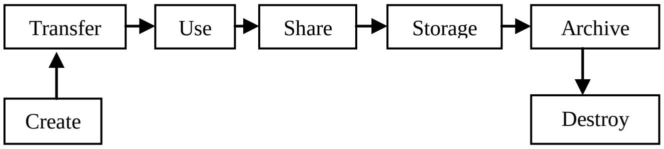

Fig 1: Data Life Cycle

• **Third-Party Control**- Cloud Service supplier is managing the user information. Third party access could cause outpouring of sensitive info and trade secrets. There’s additionally nice threat to company spying. It shouldn't additionally produce a state of affairs that user should rely upon a 1 such cloud service supplier.

- **Legal problems and Privacy**- User is unaware concerning wherever information is kept in cloud. In every country cyber laws square measure different. There's nice concern concerning lawfulness, confidentiality of knowledge. User is additionally involved concerning its information privacy. Major privacy problems associated with cloud computing square measure argus-eyed by Pearson

## II SECURITY CHALLENGES

Security, Privacy and trust square measure the most challenges or problems one got to address before reaching to develop or adopt to the cloud atmosphere because it encompasses a range of technologies together with resource sharing and allocation, cloud networks, O.S, virtualization, dealing management, encryption, concurrency management, publishing, load reconciliation and memory management, etc. Let's United States discuss intimately however completely different problems concerning to security of cloud affects customers and additionally solutions to them.

A. Authenticity/Identity Management Identity management or legitimacy of client is utmost importance in cloud since there square measure victimization the shared pool of resources and everything is accessed by alternative users if not managed properly, it refers to responsibility of supplier wherever he cannot modify the data directly and indirectly and additionally has to check for the identity of client before giving access to them. Integrity may be a major issue long-faced by the cloud atmosphere. Essence of cloud is that the information keeps at completely different geographies so transferred to alternative places associate authentic system should be in situ to confirm integrity, which may stop unauthorized users to prevent victimization data. This drawback will solved by victimization several ancient techniques like digital signatures and additionally alternative strategies projected square measure access management theme mentioned in [2] uses a suburbanized and additionally a sturdy access management mechanism wherever authentication is completed while not knowing the user's identity. By suing crypto logical Techniques info is decrypted by solely the authentic users. Alternative Systems embrace two step verification wherever a particular codes square measure sent to individual user phone to ascertain the access rights of consumers.

B. Key Management we have a tendency to mentioned coding higher than strategies mentioned especially use keys to write and also decode the data. Managing those keys additionally a serious issue in cloud since those square measure the most base of access to info. Storing keys on same cloud isn't correct and storing multiple keys becomes an oversized task. Otherwise storing it on separate information removes the most reason to decide on cloud therefore we will eliminate that choice. The answer that is best to the current drawback is by victimization 2 level coding that is mentioned in [3] for key management.

C. Trust is that the initial and foremost parameter to be addressed between client and repair provider's economical and effective use of cloud computing. client forever encompasses a doubt whether or not the service is trustworthy and additionally whether or not the personal information that is being uploaded to cloud is secure from any exploits, attackers or not. There square measure SLA's (Service Legal Agreement) which may solve this issue that is being followed from long term. SLA is associate agreement between client and supplier that describes the offerings of supplier and therefore the future plans [4]. Though this may solve the trust tissue however there are not any standards for SLA's. There has been several solutions projected to resolve trust problems in recent times a number of them square measure as follows, Trust rating mechanism is projected in [5] to secure cloud computing atmosphere with the collaboration or facilitate of social media. A Trust model is projected in [6] to boost security and trust of client and ability of cloud. A framework for SLA [7] is taken to propose a trust management model in cloud atmosphere.

D. Confidentiality is outlined as a parameter to explain the arrogance in supplier for preventing any info or information speech act. several strategies square measure rife to preserve the user confidentiality and additionally shield identity of the purchasers United Nations agency doesn't wish to be exposed, as an example coding is most generally used. Main drawback with cloud is that information is kept in several distributed locations which may be accessed by several people thanks to the unified design of cloud atmosphere. a brand new approach is projected in [8] It proposes victimization hierarchy of P2P system of name to confirm privacy. It obtains it thanks to virtualized atmosphere. To confirm privacy a secure cloud computing storage service is projected and designed with the assistance of crypto logical techniques therefore here privacy is being ensured and alternative crypto logical techniques also are developed to preserve privacy therefore giving confidentiality to customers.

E. Coding as we have a tendency to all apprehend is that the method of securing important and personal information so it will solely be accessed by users for whom it's meant. it's additionally most used technique in cloud computing. though there are several drawbacks like high computation time or alternative familiar issues with coding it's the foremost used technique and lots of strategies are developed to decrease the computation time needed for coding or coding therefore increasing output.

In [2] a brand new technique for coding is projected to boost potency and therefore shield information, "End-to-end policy primarily based write ion” is that the technique that uses completely different policies and encrypt and decode information in step with the policies. Coding keys square measure given by Trust Authority and therefore enabling the user’s to urge personal access to the clouds. Alternative strategies also are projected like Homomorphic coding which may be applied in cloud computing atmosphere security.

F. Multi residency the essence of Cloud Computing as explained higher than in introduction is Multi residency wherever completely different resources and services square measure shared all the user of the cloud atmosphere in applications, users at completely different geographic locations.

This may be done to resolve the problems of resource distribution to resolve deficiency of resources and to decrease the price to client permitting him to scale as per demand.

Therefore by sharing confidentiality of the data of various organizations are risks. Therefore isolation should be done to confirm confidentiality, else are an enormous loophole within the suppliers giving Cloud computing atmosphere should have ancient security improvement techniques combined with new technologies like Intrusion detection system to stay information safe.

G. Information ripping as we've seen that key management and coding on its own may be a tedious operation and different thereto is information ripping it's quick and additionally reliable than coding. Information ripping because the name suggests split the information over multiple hosts that square measure non-connected. Once the user got to access information, he should access all service suppliers to remember his original information.

However there square measure security problems additionally concerned. In [2] a model is projected for economical and reliable use of knowledge ripping, Multi-Cloud information Model is that the technique for information ripping wherever several clouds and lots of alternative techniques square measure wont to make sure the integrity, legitimacy of knowledge when the split of knowledge.

Therefore by victimization this technique information is keep and replicated in step with some parameters and therefore decreases intruder’s attacks on the cloud.

H. User level problems supplier should check that that thanks to accidental conduct of users information should not be lost there should be resolution to handle accidental deletion and recovery to confirm integrity and superimposed memory management and alternative problems that will arise as a result of user access to information ought to be avoided like data thieving, felonious information access as mentioned higher than etc.

I. Infected applications Service provider got to have the complete access to the server with all rights with the tip goal of perceptive and support of server. Thus this may keep any vindictive consumer from transferring any contaminated application onto the cloud which is able to extraordinarily influence the consumer and distributed computing administration.

J. Backup ancient Backup strategies that square measure getting used square measure for gift systems wherever earlier desktop or specific applications square measure used and data centres were designed for consumer’s application usage and that they cannot be all applicable to the cloud atmosphere, they're to a degree applicable however cannot be wont to completely assured concerning information recovery.

Merchant has to perpetually update the sensitive and needed info to the backup service so the information is saved just in case of any issues, and therefore the information backup should be encrypted so information won't be accessible outside the atmosphere or alternative attackers.

Generally once information is encrypted it's not simply understood by unauthorized individuals and to urge plain text back decryption is employed. For any reasonably computation one has to perform the coding initial. Coding solves major problems.

However the facility of cloud is exploited if user is ready to hold out computation on encrypted information. Homomorphic coding technique allows computing with encrypted information. It means, one is ready to perform the operations on this information while not changing into the plaintext. Information is in encrypted state in its most of the stages on the cloud.

Fully Homomorphic coding (FHE) technique permits user to perform multiple varieties of operations on encrypted information.

Only 1 reasonably operation is allowed during a part homomorphic coding technique. Fig. 2 shows the projected system.

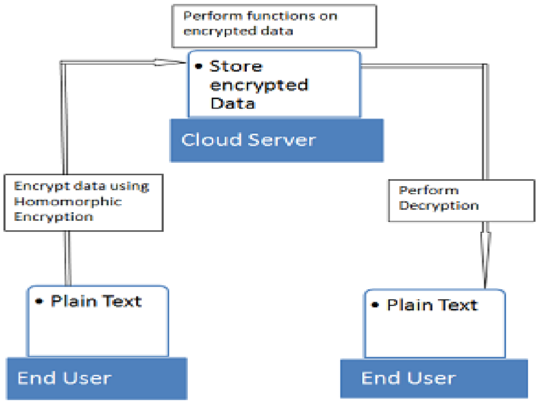

Figure 2: FHE Proposed System

## III HOMOMORPHIC ENCRYPTION

Generally, all the info holds on within the cloud is in encrypted kind. Whenever the user needs any processed knowledge, the cloud supplier decrypts that knowledge, performs computation on it and so provides the result to the user. Here comes the necessity of security because the hacker will hack the info whereas process on cloud. What if the cloud service provider doesn't decode the info whereas processing. This idea is termed Homomorphic cryptography. Figure one shows the homomorphic cryptography on cloud.

In different words, homomorphic cryptography could be a technique that permits the computation on encrypted knowledge while not previous decipherment, and once operation, if the user decrypts the result that is within the encrypted kind it provides the first result while not knowing the first plaintext [9].

Let m be a noticeable text.
Operation (m ) = decode (operation (encrypt (m ))) ...(1)

Let R + and R* be a collection of positive real numbers and set of logarithms of this set of real numbers, respectively; on these sets, the addition of real numbers and multiplication of logarithms area unit homomorphic operations (Hayes et al., 2012).

Let x, y and z □ R+
If x, y = z …(2)

Then

log(x)+ log(y)= log(z) …(3)

or

log(x)+ log(y)=log(x*y) …(4)

If we tend to take antilogarithm of the log (z), then we tend to get original z, i.e., result.

The on top of example provides America 2 ways in which to seek out z, i.e., either directly or through logarithms. In each case, we tend to get a similar result. Therefore, rather than acting operation on plain text, it's safer to perform it on encrypted knowledge.

Figure a pair of shows that the homomorphic cryptography works on integers by taking random rule. For cryptography, rule is employing a technique, i.e., number is multiplied by a pair of. Like 7*2 = fourteen and 3*2 = half-dozen once cryptography.

Decryption rule works in reverse order, i.e., once multiplication of encrypted knowledge, divide it by a pair of, i.e., (14*6)/2 = forty two. As a result of the rule has homomorphic cryptography property, once decipherment of the result, we tend to get original results of multiplication, i.e., 7*3 = 21
.
Figure three shows the homomorphic cryptography works on strings by taking random technique.

## IV.RELATED WORK

**Rivest et al. (1978)** introduced for the primary time the conception of Homomorphic secret writing. Taher (1985) introduced associate algorithmic program supported increasing property. Paillier (1999) planned associate algorithmic program referred to as Pailler cryptosystem that has additive homomorphic property and there square measure varied applications, there this technique is enforced like e-voting, etc.

**Chan (2009)** works on privacy homomorphy within which we will perform operation on encrypted knowledge. They need given 2 additive homomorphic schemes: Iterated Hill Ciper and changed RSA. The varied homomorphic secret writing schemes planned by totally different researchers square measure bestowed in Table one.

**Shahzadi et al. (2012)** has done the elaborate study of 3 homomorphic secret writing algorithms, i.e., RSA, El Gamal and Paillier. They need evaluated all 3 algorithms and Shown the comparative study between them. The result shows that RSA performs higher than El Gamal and Paillier and El Gamal Performs higher than Paillier.

**Naser and Bin (2013)** surveyed on specific security problems and use of cryptography in cloud computing. Taurus et al. (2013) mentioned concerning the recent advances in homomorphic secret writing techniques. they need done survey on recent advances in Somewhat Homomorphic secret writing (SWHE) and totally Homomorphic secret writing (FHE) algorithms.

**Ramgovind et al. (2010)** highlighted key security issues presently faced by trade. Aderemi and Oluwaseyi (2011) mentioned concerning the protection problems in cloud computing and therefore the potentials of homomorphic secret writing, associated planned a secret writing layer on prime of the encrypted knowledge on the cloud.

**Liu (2012)** has introduced some cloud system and conjointly analyses cloud computing security drawback. He recommended that single security technique cannot be wont to solve the cloud security drawback so, several ancient and a few new methods square measure needed to use along to produce the entire security in cloud.

**Ustimenko and Wroblewska (2013)** planned an inspiration for homomorphic secret writing and variable key for cloud security [10]. They need given elaborate discussion on Key Dependent Message (KDM) secret writing theme is used for cloud security.

### V. CONCLUSION AND FUTURE WORK

Homomorphic secret writing can bring a replacement dimension to cloud storage. It provides confidentiality to the information as in no stage knowledge is exposed in plain text. The planned algorithmic program is simplified, economical version applied in AWS public cloud. The planned algorithmic program is used for varied applications like on-line auctioning, medical purposes and business functions.

There is got to perform analysis in reducing the dimensions of cipher text for economical processing. There's conjointly a need to evolve varied algorithms for looking out and querying on encrypted knowledge underneath FHE theme.

## REFERENCES

[1]. S.L.Mewada, U.K. Singh, P. Sharma, "*Security Enhancement in Cloud Computing (CC)*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.31-37, 2013. Yu, Shucheng, "Achieving secure, scalable and first-class-grained know-how access management in cloud computing." INFOCOM, 2010 Proceeding IEEE, 2010.

[2]. Pearson, Siani, "*Taking account of privacy as soon as planning cloud computing offerings*." Proceedings of the 2009 ICSE Workshop on software program package Engineering Challenges of Cloud Computing, IEEE Society, 2009.

[3]. M. Al. Zain, B. Soh, & E. Pardede, "*Replacement Approach victimization Redundancy Technique to reinforce Security*" in Cloud Computing, IEEE, 2012

[4]. R.Piplode, P. Sharma and U.K. Singh, "*Study of Threats, Risk and Challenges in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.26-30, 2013.

[5]. Hwang, Kai, Sameer Kulkareni, and Yue Hu, *"Cloud safety with virtualized defines and popularity-primarily based receive as true with manipulate."* Dependable, involuntary and Secure Computing, International Conference on IEEE, 2009.

[6]. V.P.Muthukumar and R.Saranya, "*A Survey on Security Threats and Attacks in Cloud Computing*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.11, pp.120-125, 2014.

[7]. Wooten, Ryan, "*Design and implementation of a at ease useful resource social cloud system*." Cluster, Cloud and Grid Computing (CC Grid), 2012 twelfth IEEE/ACM International convention, IEEE, 2012.

[8]. Ahlam Ansari, Tahir Ansari, Faizan Hingora and Mudassir Ansari, "*A Secure Cloud Server Using Raspberry Pi and Kerberos Authentication Protocol*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.3, pp.56-58, 2015.

[9]. Vivek Raich, Pradeep Sharma, Shivlal Mewada and Makhan Kumbhkar, "*Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.6, pp.13-16, 2013.

**Authors Profile**

Abhishek Satyarthi,pursued Bachlors of engineering From LNCT, Bhopal (MP), India in 2014. He is currently pursuing his Master of Engineering from Madhav Institute of Technology and Science,Gwalior (MP), India

Sanjiv Sharma PhD, M.Tech(IT), B.E.(IT) is an Assistant Professor in the Department of Computer Science Engineering and Information Technology at Madhav Institute of Technology & Science Gwalior (MP), India. He received his PhD degree (Computer Science & Engineering) from Banasthali University, Jaipur (Raj.), India in 2014 and M.Tech (Information Technology) with honors from School Of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal(MP), India in 2007. His current research interests include Social Network Analysis, Data Mining, Network Security, Adhoc Network and Mobile Computing and their interdependency.