International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

HOMOMORPHIC ENCRYPTION SCHEME IN CLOUD COMPUTING FOR SECURITY AND PRIVACY OF SENSITIVE DATA

Mrs.Soniya Bastwade[1], Ms. Neha D.Patil[2]

[1,2]*Asst. Prof, Dept. of Computer Engg, D.Y. Patil COE, Pune, Maharashtra, India*

Abstract – *Nowadays privacy of our own sensitive data becomes the highest priority for people. Generally, we offer knowledge security and privacy protection through encrypted knowledge however at the expense of usability. Absolutely homomorphic cryptography permits to perform unlimited chaining of mathematical operations on encrypted knowledge creating it more secure for a few legal corporations and establishments to use it. Encryption technology can provide data privacy security in cloud environment, but there are many problems in the process of access the data which is encrypted, because at the time of accessing encrypted data there are chances to leak our sensitive data which can be avoided into homomorphic encryption techniques.*

KeyWords: Cloud Computing, Security, Homomorphic, Encryption.

1. INTRODUCTION

Cloud computing is revolutionizing several of our ecosystems, together with aid. Compared with earlier ways of process information, cloud computing environments offer vital edges, like the provision of automatic tools to assemble, connect, tack and reconfigure virtualized resources on demand. These build it abundant easier to satisfy structure goals as organizations will simply deploy cloud services. However, the shift in paradigm that accompanies the adoption of cloud computing is more and more giving rise to security and privacy concerns regarding aspects of cloud computing like multi-tenancy, trust, loss of management and responsibleness [1]. Consequently cloud platforms that handle sensitive info square measure needed to deploy technical measures and structure safeguards to avoid information protection breakdowns which may end in monumental and expensive damages. Data privacy in cloud computing may be elementary issue nowadays. Absolutely homomorphic codin g schemes area unit extremely counseled for knowledge security in cloud computing. In fact, confidentiality of smart knowledge will be preserved although a non-trusted cloud server processes it; the mystery behind this can be that absolutely homomorphic coding schemes permit process encrypted knowledge while not the necessity of a previous coding. During this paper we have a tendency to gift a brand new absolutely homomorphic coding theme from integers. Our coding theme will be used primarily to secure smart knowledge in cloud computing. The planned theme uses an oversized whole number ring as clear text house and one key for coding and coding, i.e. it's a isosceles coding theme. Isosceles coding may be a kind of processed cryptography employing a singular coding key to colour associate electronic mail. Its conversion uses a mathematical algorithmic rule together with a secret key, which ends within the inability to create sense out of a message. Isosceles coding may be a two-way algorithmic rule as a result of the mathematical algorithmic rule is reversed once decrypting the message together with mistreatment a similar secret key. Isosceles coding is additionally referred to as private-key coding and secure-key coding.

LITERATURE REVIEW

Authentication and Authorization

In [6] the authors propose a credential classification and a framework for analyzing and developing solutions for credential management that include strategies to evaluate the complexity of cloud ecosystems. This study identifies a set of categories relevant for authentication and authorization for the cloud focusing on infrastructural organization which include classifications for credentials, and adapt those categories to the cloud context. The study also summarizes important factors that need to be taken into consideration when adopting or developing a solution for authentication and authorization – for example, identifying the appropriate requirements, categories, services, deployment models, lifecycle, and entities.

In other work, a design model for multi-factor authentication in cloud computing environments is proposed in [7], and this model includes an analysis of the potential security threats in the proposed model. Another authentication solution is seen with MiLAMob [8], which provides a SaaS authentication middleware for mobile consumers of IaaS cloud applications. MiLAMob is a middleware-layer that handles the real-time authentication events on behalf of consumer devices with minimal HTTP traffic. The middleware currently supports mobile consumption of data on IaaS clouds such as Amazon's S3.

Identity and Access Management

The important functionalities of identity management systems for the success of clouds in relation to consumer satisfaction is discussed in [9]. The authors also present an authorization system for cloud federation using Shibboleth - an open source implementation of the security assertion mark-up language (SAML) for single sign-on with different cloud providers. This solution demonstrates how organizations can outsource authentication and authorization to third party clouds using an identity management system. Stihler et al. [10] also propose an integral federated identity management for cloud computing. A trust relationship between a given user and SaaS domains is required so that SaaS users can access the application and resources that are provided. In a PaaS domain, there is an interceptor that acts as a proxy to accept the user's requests and execute them. The interceptor interacts with the secure token service (STS), and requests the security token using the WS-Trust specification.

Confidentiality, Integrity, and Availability

Santos et al. [11] extend the Terra [12] design that enables users to verify the integrity of VMs in the cloud. The proposed solution is called the trusted cloud computing platform (TCCP), and the whole IaaS is considered to be a single system instead of granular hosts in Terra. In this approach, all nodes run a trusted virtual machine monitor to isolate and protect virtual machines. Users are given access to cloud services through the cloud manager component. The external trusted entity (ETE) is another component that provides a trust coordinator service in order to keep track of the trusted VMs in a cluster. The ETE can be used to attest the security of the VMs. A TCCP guarantees confidentiality and integrity in data and computation and it also enables users to attest to the cloud service provider to ensure whether the services are secure prior to setting up their VMs. These features are based on the trusted platform module (TPM) chip. The TPM contains a private endorsement key that uniquely identifies the TPM and some cryptographic functions that cannot be altered.

Security Policy Management

In [13] the authors propose a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies through a policy management module. The user activities are stored and monitored for each storage system, and are made available to the policy management module. Users' actions are evaluated by a trust management module based on their past activities and are grouped as "fair" or "malicious". An appropriate architecture for security management which satisfies the requirements of policy definitions (such as flexibility, expressiveness, extendibility and correctness) has been implemented. The authors evaluated the proposed system on a data management system that is built on data storage. Takabi et al. [14] introduce policy management as a service (PMaaS) to provide users with a unified control point for managing access policies in order to control access to cloud resources independently of the physical location of cloud providers. PMaaS is designed specifically to solve the issue of having multiple access control authorization mechanisms employed by cloud service providers that restrict the flexibility of applying custom access control to a particular service. For this purpose, the PMaaS architecture includes a policy management service provider that is the entry point for cloud users to define and manage the policies. The cloud service provider imports the user-defined policies and acts a policy decision point to enforce the user policies.

PROBLEM STATEMENT

Statement 1:

In order to construct secure protocol for electronic voting. In election schemes, the homomorphic property provides a tool to obtain the tally given the encrypted votes without decrypting the individual votes and discovering voters' identities and their personal tendency.

Statement 2:

To allow business users to perform multiple operations over data, stored in cloud data centres, without need of huge calculations on client' side.

Statement 3:

Possibly lower expenses, while ensuring customer's data privacy.

Statement 4:

To avoid the data leakage and provide confidentiality of sensible data can be preserved even if a non trusted cloud server processes.

Statement 5:

To allow processing encrypted data without the need of a prior decryption.

Homomorphic Encryption:

In cloud computing the major concern is about the privacy risks, because when we are storing data in cloud it will be in encrypted format and cloud computers knows what actually a client data is. So if the hacker get the data access then he can see all the data stored by client on cloud. It menace if we are using simple cloud computing technique to store and secure our data then there are chances to leak our data and accessed by any unauthorized person. Following fig.1 . Shows the functioning of cloud computing.

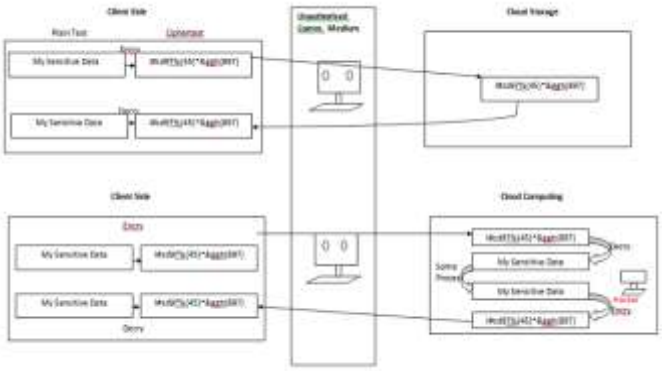

Fig.1: Cloud computing Technique

In homomorphic encryption cloud computers doesn't know about data stored by clients on cloud storage. In this process we can do the homomorphic operations where we can decrypt the data without showing the original data even to cloud computers. So there is no chance to leak our sensitive data nad cannot be accessed by any other unauthorised person. Fig 2 shows how homomorphic Encryption works.

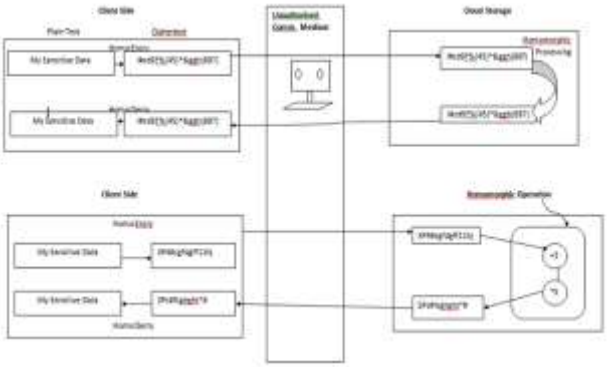

Fig 2. Homomorphic Encryption Technique.

EXPECTED OUTCOME

An attack algorithm on the symmetric homomorphic encryption scheme proposed by Li et al. Our attack can recover the secret key from two plaintext/cipher text pairs. The computational complexity of our attack is O (log4p). To recover the entire secret key in the generated instances in several seconds when the number of homomorphic multiplications is greater than 2.

Symmetric algorithm randomizes messages into integers. It is a noise free and probabilistic FHE scheme from integers, it can be used for data security in cloud computing. The security of this algorithm is based on the problem of factorization of big numbers.

METHODOLOGY TO BE USE

Cloud Computing with Application in private queries to a search engine, searching over encrypted data, private information retrieval(PIR), protocol PIR allows him to retrieve his wanted information's in a safer way and without the cloud server being able to determine which element was selected, protection of mobile agents against malicious hosts by encrypting them, secure protocol for electronic voting, and also in n traditional approach of advertisement, a mobile device sends a user's location to a provider, who sends customized ads, such as discount vouchers for nearby shops, back to the user.

REFERENCES

[1] R. Rivest, L. Adleman and M. Dertouzos, "On Data Banks and Privacy Homorphisms," In Foundataions of Secure Computataion,Academic Press, pp. 169-179, 1978.

[2] C. Gentry, "A fully homomorphic encryption scheme,"https://crypto.stanford.edu/craig/craig-thesis.pdf, September 2009.

[3] K. Lauter, M. Naehrig et V. Vaikuntanathan, «Can homomorphic encryption be practical?,»available athttps://eprint.iacr.org/2011/405.pdf.

[4] Z. Brakerski et V. Vaikantanathan, " Efficient Fully HomomorphicEncryption from (Standard) LWE", Available at http://eprint.iacr.org/2011/344.

[5] C. Gentry, S. Halevi et N. Smart, "Fully Homomorphic Encryption with Polylog Overhead," available athttps://eprint.iacr.org/2011/566.pdf.

[6] N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[7] R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for cloud computing," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[8] R. Lomotey and R. Deters, "Saas authentication middleware for mobile consumers of iaas cloud," in Services (SERVICES), 2013 IEEE Ninth World Congress on, pp. 448–455, June 2013.

[9] M. A. Leandro, T. J. Nascimento, D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Multitenancy authorization system with federated identity for cloud-based environments using shibboleth," in Proceedings of the 11th

International Conference on Networks, ICN 2012, pp. 88–93, 2012.

[10] M. Stihler, A. Santin, A. Marcon, and J. Fraga, "Integral federated identity management for cloud computing," in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, pp. 1–5, May 2012.

[11] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.
[12] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, SOSP '03, (New York, NY, USA), pp. 193–206, ACM, 2003.

[13] C. Basescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing data access on clouds: A generic framework for enforcing security policies," in Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, pp. 459–466, March 2011.

[14] H. Takabi and J. Joshi, "Policy management as a service: An approach to manage policy heterogeneity in cloud computing environment," in System Science (HICSS), 2012 45th Hawaii International Conference on, pp. 5500–5508, Jan 2012.