A review of homomorphic encryption of data in cloud computing

Dr. Amit Chaturvedi [#1], Akanksha Kapoor [*2], Dr. Vikas Kumar [#3]

[#1] *Assistant Prof., Govt. Engineering College, Ajmer*
[*2] *M.Tech. Scholar, Bhagwant Univ., Ajmer, India*

Abstract - *The term encryption refers to converting the original data into human unreadable form (encoding). The conversion of the encoded data into original form is known as decryption. By encrypting the data only the authorized person can decode the original data. Thus data confidentiality is achieved by the encryption. In this paper, we reviewed the algorithms proposed for the homomorphic encryption of data in cloud computing.*

Keywords – *encryption, homomorphic, cloud, security.*

I. INTRODUCTION

Cloud computing has gained tremendous popularity in recent years. By outsourcing computation and storage requirements to public providers and paying for the services used, customers can relish upon the advantages of this new paradigm. Cloud computing provides with a comparably lower-cost, scalable, a location-independent platform for managing clients' data. Compared to a traditional model of computing, which uses dedicated in-house infrastructure, cloud computing provides unprecedented benefits regarding cost and reliability. Cloud storage is a new cost-effective paradigm that aims at providing high availability, reliability, massive scalability and data sharing. However, outsourcing data to a cloud service provider introduces new challenges from the perspectives of data correctness and security. Over the years, many data integrity schemes have been proposed for protecting outsourced data.

This new model has gained tremendous popularity and is receiving a lot of attention from researchers in the academic and industrial communities. Essential characteristics of the cloud-computing model include on-demand self-service, rapid elasticity, resource pooling and broad network access. Cloud computing has gained a lot of popularity, which is mainly due to the following reasons : (a) Cloud computing has eliminated the overhead of planning from the user, providing resources that are available on-demand, self-service, and the ability to scale according to requirements. (b) Cloud computing has eliminated up-front commitment by the end users. Pay-as-you-go model has allowed companies to start small and increase their computing resources only when needed.

Information security architectures typically presume the ability to erect perimeters, both physical and logical, around areas of trust and control. An institution can control the flow of their information by controlling when and how information crosses boundaries. In the cloud environment parts of the perimeter move to the cloud and institutions must trust the cloud infrastructure provider for perimeter control maintenance. In this sense, from a security perspective, cloud computing follows on in the tradition of de-perimeterisation problems.

The main draws of cloud computing include, its configurability, availability and ease of support. Draft-NIST-SP800-146 defines cloud computing as: "a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Badger et al., 2011).

II. RELATED WORK

M. M. Poteya , Dr C. A. Dhoteb, D. H. Sharma discussed Homomorphic Encryption for Security of Cloud Data. Cloud computing is a broad and diverse phenomenon. Users are allowed to store large amount of data on cloud storage for future use. The various security issues related to data security, privacy, confidentiality, integrity and authentication needs to be addressed. Most of the cloud service provider stores the data in plaintext format and user need to use their own encryption algorithm to secure their data if required. The data needs to be decrypted whenever it is to be processed. This paper focuses on storing data on the cloud in the encrypted format using fully homomorphic encryption. The data is stored in DynamoDB of Amazon Web Service (AWS) public cloud. User's computation is performed on encrypted data in public cloud. When results are required they can be downloaded on client machine. In this scenario users data is never stored in plaintext on public cloud.

M.Teeba, S.E. Hajii proposed that Go to the cloud, has always been the dream of man. Cloud Computing offers a number of benefits and services to its customers who pay the use of hardware and

software resources (servers hosted in data centers, applications, software...) on demand which they can access via internet without the need of expensive computers or a large storage system capacity and without paying any equipment maintenance fees.

B.K. Mohanta, D. Gountia stated that As the data storage challenge continues to grow for insurers and everyone else, one of the obvious solutions is cloud technology. Storing data on remote servers rather than in-house is definitely a money-saver, but in insurance circles, the worry has been that having critical data reside outside the physical and virtual walls of the insurance enterprise is a risky situation. As the IT field is rapidly moving towards Cloud Computing, software industry's focus is shifting from developing applications for PCs to Data Centers and Clouds that enable millions of users to make use of software simultaneously.

S. Bajpai and P. Srivastava presented that Cloud Computing has been the most promising innovation in the computing world in past decade. Its usage is still hindered by the security concerns related with critical data. The encryption of remotely stored data has been the most widely used technique to bridge this security gap. The speculated vast usage of Cloud Computing solutions for data storage and with Big Data Analytics gaining strong foothold; the security on cloud is still at big risk. Fully Homomorphic Encryption is a good basis to enhance the security measures of un-trusted systems or applications that stores and manipulates sensitive data. The model is proposed on cloud computing which accepts encrypted inputs and then perform blind processing to satisfy the user query without being aware of its content, whereby the retrieved encrypted data can only be decrypted by the user who initiates the request. This allows clients to rely on the services offered by remote applications without risking their privacy.

D. Dave,R. Thakkar proposed that Cloud computing is the most important parameter of distributed computing. Cloud computing ore use and its easily available services at low cost. Cloud computing provide data security. Now a day's data security and confidentiality is the major issues. In this paper focus on solve the security and confidentiality problem. Homomorphic encryption is the best solution of this problem. In this paper new technique homomorphic apply and solve the security and confidentiality problem.

K. Benzekki, A. E. Fergougui, and A. E. B. E. Alaoui presented that The Purpose of homomorphic encryption is to ensure privacy of data in communication, storage or in use by processes with mechanisms similar to conventional cryptography, but with added capabilities of computing over encrypted data, searching an encrypted data, etc. Homomorphism is a property by which a problem in one algebraic system can be converted to a problem in another algebraic system, be solved and the solution later can also be translated back effectively. Thus, homomorphism makes secure delegation of computation to a third party possible. Many conventional encryption schemes possess either multiplicative or additive homomorphic property and are currently in use for respective applications. Yet, a Fully Homomorphic Encryption (FHE) scheme which could perform any arbitrary computation over encrypted data appeared in 2009 as Gentry's work. In this paper, we propose a multi-cloud architecture of N distributed servers to repartition the data and to nearly allow achieving an FHE.

M. TEBAA, S.E. HAJJI, A. E. GHAZI discussed that Cloud computing security challenges and it's also an issue to many researchers; first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud. The advantages of cloud computing include reduced costs, easy maintenance and re-provisioning of resources, and thereby increased profits. But the adoption and the passage to the Cloud Computing applies only if the security is ensured. How to guaranty a better data security and also how can we keep the client private information confidential? There are two major questions that present a challenge to Cloud Computing providers.

When the data transferred to the Cloud we use standard encryption methods to secure the operations and the storage of the data. But to process data located on a remote server, the Cloud providers need to access the raw data. In this paper we are proposing an application of a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data.

HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, FU Jing-yi, and NIU Xin-xin proposed "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing". Cloud computing provides a convenient way of content trading and sharing. In this paper, they propose a secure and privacy-preserving digital rights management (DRM) scheme using homomorphic encryption in cloud computing. We present an efficient digital rights management framework in cloud computing, which allows content provider to outsource encrypted contents to centralized content server and allows user to consume contents with the license issued by license server. Further, we provide a secure content key distribution scheme based on additive homomorphic probabilistic public key encryption and proxy re-encryption. The provided scheme prevents

malicious employees of license server from issuing the license to unauthorized user. In addition, we achieve privacy preserving by allowing users to stay anonymous towards the key server and service provider. The analysis and comparison results indicate that the proposed scheme has high efficiency and security.

Xiaofen Wang discussed One-round secure fair meeting location determination based on homomorphic encryption. This paper states that determination of optimal meeting location without revealing the locations of participants to the location server is an interesting research problem. A major concern for a location based service is location privacy. However, adding privacy protection to a location service will inevitably introduce computational complexity. To provide location privacy with low computational cost is a challenging task. In this paper, we propose a one-round meeting location determination protocol, where the location service provider makes a decision with a semi-trusted cloud server which works as a computation centres and conducts most of computation. The user location privacy is preserved against the outside and internal attackers including the computation center, the meeting location determination server and participants. In order to study the performance of the protocol, we test its computational efficiency on smartphones. The simulation results and the performance comparison of our protocol with another protocol of the same functionalities demonstrate that our solution is more efficient and practical.

S. Dasgupta, S.K. Pal proposed Design of a polynomial ring based symmetric homomorphic encryption scheme. Security of data, especially in clouds, has become immensely essential for present-day applications. Fully homomorphic encryption (FHE) is a great way to secure data which is used and manipulated by untrusted applications or systems. In this paper, we propose a symmetric FHE scheme based on polynomial over ring of integers. This scheme is somewhat homomorphic due to accumulation of noise after few operations, which is made fully homomorphic using a refresh procedure. After certain amount of homomorphic computations, large ciphertexts are refreshed for proper decryption. The hardness of the scheme is based on the difficulty of factorizing large integers. Also, it requires polynomial addition which is computationally cost effective. Experimental results are shown to support our claim.

F. Farokhi, I. Shames, N. Batterham discussed Secure and Private Cloud-based control using semi-homomorphic encryption. Networked control systems with encrypted sensors measurements is considered. Semi-homomorphic encryption is used so that the controller can perform the required computation on the encrypted data. Specifically, in this paper, the Paillier encryption technique is utilized that allows summation of decrypted data to be performed by multiplication of the encrypted data. Conditions on the parameters of the encryption technique are provided that guarantee the stability of the closed-loop system and ensure certain bounds on the closed-loop performance.

Z. Wang, G. Sun, D. Chen presented A new definition of homomorphic signature for identity management in mobile cloud computing. In this paper, we define a new homomorphic signature for identity management in mobile cloud computing. A mobile user firstly computes a full signature on all his sensitive personal information (SPI), and stores it in a trusted third party (TTP). During the valid period of his full signature, if the user wants to call a cloud service, he should authenticate him to the cloud service provider (CSP) through TTP. In our scheme, the mobile user only needs to send a {0, 1}n vector to the access controlling server (TTP). The access controlling server who doesn't know the secret key can compute a partial signature on a small part of user's SPI, and then sends it to the CSP. We give a formal secure definition of this homomorphic signature, and construct a scheme from GHR signature. We prove that our scheme is secure under GHR signature.

Saravana K.N., Rajya Lakshmi G.V., Balamurugan B., discussed Enhanced Attribute Based Encryption for Cloud Computing. Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number of real times and business related cloud applications compared to consumer related cloud application. Firstly, the pros and cons of different Attribute Based encryption methods are analysed. Secondly, a new encryption method based on Attribute Based Encryption (ABE) using hash functions, digital signature and asymmetric encryptions scheme has been proposed. Our proposed algorithm is simplified yet efficient algorithm that can implemented for cloud critical application.

Vu Mai, I. Khalil proposed Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. Smart grids introduce many outstanding security and privacy issues, especially when smart meters are connected to public networks, creating an Internet of things in which customer usage data is frequently exchanged and processed in large volumes. In this research, we propose a cloud-based data storage and processing model with the ability to preserve user privacy and confidentiality of smart meter data in a smart grid. This goal is achieved by encrypting smart meter

data before storage on the cloud using a homomorphic asymmetric key cryptosystem. By applying the homomorphic feature of the cryptographic technique, we propose methods to allow most of the computing works of calculating customer invoices based on total electricity consumption to be done directly on encrypted data by the cloud. One of the outstanding features in our model is the aggregation of encrypted smart meter readings using fixedpoint number arithmetic. To test the feasibility of our model, we conducted many experiments to estimate the number of homomorphic additions to be performed by the cloud and the computation time in different billing periods using data from the Smart project, in which smart grid readings were continuously collected from different households in every second within two months and electricity usage data collected every minute from 400 anonymous houses in one day. We also propose a parallel version of our billing algorithm to utilize the processing capability of multi-core processors in cloud servers so that computation time is reduced significantly compared to using our sequential algorithm. Our research works and experiments demonstrate clearly how cloud services can strengthen the security, privacy and efficiency of privacy-sensitive data frequently exchanged and processed in an Internet of things where smart meters communicate directly with public networks.

S. Singh, Y.S. Jeong, J.H. Park presented A survey on cloud computing security: Issues, threats, and solutions. Over the internet, the cloud computing reveals a remarkable potential to provide on-demand services to consumers with greater flexibility in a cost effective manner. While moving towards the concept of on demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. This survey present a comprehensive overview of the security issues for different factors affecting cloud computing. Furthermore, a detailed discussion on several key topics regarding embedded system, application, storage system, clustering related issues and many more. This paper works on some public cloud and private cloud authorities as well as related security concerns. Additionally, it encompasses the requirements for better security management and suggests 3-tier security architecture. Open issues with discussion in which some new security concepts and recommendations are also provided.

F. Chao, X.Yang proposed Fast key generation for Gentry-style homomorphic encryption. The key issue of original implementation for Gentry-style homomorphic encryption scheme is the so called slow key generation algorithm. Ogura proposed a key generation algorithm for Gentry-style somewhat homomorphic scheme that controlled the bound of the evaluation circuit depth by using the relation between the evaluation circuit depth and the eigenvalues of the primary matrix. However, their proposed key generation method seems to exclude practical application. In order to address this problem, a new key generation algorithm based on Gershgorin circle theorem was proposed. The authors choose the eigenvalues of the primary matrix from a desired interval instead of selecting the module. Compared with the Ogura's work, the proposed key generation algorithm enables one to create a more practical somewhat homomorphic encryption scheme. Furthermore, a more aggressive security analysis of the approximate shortest vector problem (SVP) against lattice attacks is given. Experiments indicate that the new key generation algorithm is roughly twice as efficient as the previous methods.

S. K. Pasupuleti, S. Ramalingum, R. Buyya proposed an efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Outsourcing of data into cloud has become an effective trend in modern day computing due to its ability to provide low-cost, pay-as-you-go IT services. Although cloud based services offer many advantages, privacy of the outsourced data is a big concern. To mitigate this concern, it is desirable to outsource sensitive data in an encrypted form but cost of encryption process would increase the heavy computational overhead on thin clients such as resource-constrained mobile devices. Recently, several keyword searchable encryption schemes have been described in the literature. However, these schemes are not effective for resource-constrained mobile devices, because the adopted encryption system should not only support keyword search over the encrypted data but also offer high performance. In this paper, we propose an efficient and secure privacy-preserving approach for outsourced data of resource-constrained mobile devices in the cloud computing. Our approach employs probabilistic public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. We aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the file retrieval accuracy. As a result, data privacy ensures and computation, communication overheads in reduction. Thorough security and performance analysis, we prove that our approach is semantically secure and efficient.

III. FINDINGS

In cloud computing, the data is place on the third party servers, and the customer is totally unaware about the location of the server. The handling of data, at the server side, is totally in the third party control. Then the cryptography techniques may improve the security level of data. From the customers/ organizations point of view, data needs to be encrypted while being stored on the cloud. Cloud servers should be able to compute on encrypted data and so the queries should be answered on the basis of encrypted data and hence the responses are also the encrypted data.

But this implementation requires the followings:

- Users must have access accounts on the cloud
- Request the cloud to perform computation on encrypted meter readings
- Decrypt and view the results
- Data needs to be encrypted before sending to be saved on the cloud servers
- There should be a defined timeline for each operations like encrypting data, decrypting data, saving a transaction on the server, etc.[14]

In their work, Deng et al. describe in detail how smart meters can register and authenticate their identities before a secure communication session can be set up with the data collector. These operations help to build a network of smart meters organized as an aggregation tree in which the data collector is the root node with information relating to the network structure and routing backbone. The author assume that smart meters are connected to one another and readings from one meter have to travel to other meters to reach the data collector. This feature is significantly different from our model in which each meter are independent and connected directly to the grid operator.[12]

Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number of real times and business related cloud applications compared to consumer related cloud application. Attribute Based encryption methods are analysed. using hash functions, digital signature and asymmetric encryptions scheme may be better model for implementation. [13]

IV. CONCLUSION

Homomorphic encryption for improving privacy of data in cloud computing is a good way for security the data. There are various algorithms proposed for encryption in cloud computing. The attribute based encryption is a proven algorithm for cloud computing environment. Ogura proposed a key generation algorithm for Gentry-style somewhat homomorphic scheme that controlled the bound of the evaluation circuit depth by using the relation between the evaluation circuit depth and the eigenvalues of the primary matrix. However, their proposed key generation method seems to exclude practical application. Specifically, the eigenvalues should be sufficiently large, which affects the efficiency of the key generation procedure.

F.Chao, and X Yang had proposed a fast key generation for Gentry-style homomorphic encryption. The future work is to decrease the eigenvalues and improve the efficiency of the key generation algorithm.

REFERENCES

[1]. M. M. Poteya , Dr C. A. Dhoteb, D. H. Sharma, "Homomorphic Encryption for Security of Cloud Data", 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016), pp. 175 – 181

[2]. M.Teeba, S.E. Hajii, "Secure Cloud Computing through Homomorphic Encryption", International Journal of Advancements in Computing Technology(IJACT), Volume5, Number16, December 2013, pp. 29-38

[3]. B.K. Mohanta, D. Gountia, "Fully homomorphic encryption equating to cloud security: An approach", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 2 (Jan. - Feb. 2013), PP 46-50

[4]. S. Bajpai and P. Srivastava, "A Fully Homomorphic Encryption Implementation on Cloud Computing", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 811-816

[5]. D. Dave,R. Thakkar, "HOMOMORPHIC ENCRYPTION IN CLOUD COMPUTING", 2015, IJIRT , Volume 1 Issue 12, ISSN: 2349-6002, pp. 1352-1357.

[6]. K. Benzekki, A. E. Fergougui, and A. E. B. E. Alaoui," A Secure Cloud Computing Architecture Using Homomorphic Encryption", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016, pp. 293-298

[7]. M.Teeba, S.E. Hajii, A.E.Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol I, ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[8]. HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, FU Jing-yi, and NIU Xin-xin, "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing", The Journal of China Universities of Posts and Telecommunications, December 2013, 20(6): 88–95.

[9]. Xiaofen Wang, "One-round secure fair meeting location determination based on homomorphic encryption", Information Sciences 372 (2016) 758–772

[10]. S. Dasgupta, S.K. Pal," Design of a polynomial ring based symmetric homomorphic encryption scheme", Perspectives in Science (2016) 8, 692—695

[11]. F. Farokhi, I. Shames, N. Batterham, "Secure and Private Cloud-based control using semi-homomorphic encryption", IFAC-PapersOnLine 49-22 (2016) 163–168

[12]. Z. Wang, G. Sun, D. Chen," A new definition of homomorphic signature for identity management in mobile cloud computing", Journal of Computer and System Sciences 80 (2014) 546–553

[13]. Saravana K.N., Rajya Lakshmi G.V., Balamurugan B.," Attribute Based Encryption for Cloud Computing", International Conference on Information and

Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 689 – 696

[14]. Vu Mai, I. Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography", Future Generation Computer Systems, 2016, 0167-739X,

[15]. S. Singh, Y.S. Jeong, J.H. Park, "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications 75 (2016), pp. 200–222

[16]. F. Chao, X.Yang, "Fast key generation for Gentry-style homomorphic encryption", The Journal of China Universities of Posts and Telecommunications, December 2014, 21(6): pp. 37–44

[17]. S. K. Pasupuleti, S. Ramalingum, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications 64 (2016) pp. 12–22