International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 249-252 www.ijaem.net ISSN: 2395-5252

A Review on Cloud Data Storage Security Using Cryptographic Technique

Kiran Yadav 1,Ajitabh Mahalkari2
Sdbct Indore A B Road Rau

Submitted: 02-01-2022 Revised: 09-01-2022 Accepted: 12-01-2022

ABSTRACT—The rapid expansion and growth of technology empowers the digitization of data to keep preserve the data for log time. Additionally the traditional computing and storage techniques are also replaced with the cloud storage and computing solutions. However the cloud is a secure and efficient infrastructure but the content delivery is often performed with the unsecure networks. In this context we need to investigate the different techniques and models which can enable us the full proof security against the network security threats. Therefore in this paper we are proposing to review the recent techniques and contributions in the domain of secure data communication between server and end cloud client. In addition, a secure data communication model has also been presented for design and implementation for cloud client for secure data delivery to target users. Finally the conclusion has been made and the future work has been reported.
Keywords—data security, cloud storage, cryptographic security, data verification, data sharing and communication, un-trusted networks, key exchange.

I. INTRODUCTION

In this age internet is become a popular medium for communication, data sharing, storage and distribution/publishing. Almost every person in this world now in these days taking the services using the internet, for example for banking, e-commerce, online meeting and many more. During these events the significant amount of data has been generated and communicated to the target servers. However these servers are full of security features such as anti-virus, firewall and other security techniques. But during communication between server to server and server to client systems are utilizing the un-trusted networks. The un-trusted networks are prone to security threats and various kinds of attacks.

Therefore, in order to secure the communication among two parties we require the different security that are able to deliver the data securely and also validate the data is not altered in the network. In this context different kinds of cryptographic techniques are incorporated for securing the communication between the client and server. But all the cryptographic techniques are not much secure or efficient. Therefore a new security model is required that provides end to end security between client and server communication. However, the cryptographic techniques are providing the security in low cost and less maintenance but the secure key exchange is a key issue in the cryptographic scenarios.

Therefore the proposed work is motivated to investigate the different cryptographic security techniques which can be utilized during the communication or transfer of data between client and server. Additionally having a security check which enable us to vilify the data is intercepted between servers or not by using the integrity check. Secondly the aim is also including locating such method that can handle the entire key management at server side and not disclose any one for encryption and decryption using the third party key management service. This section provides only the basic overview of the proposed concept, additionally key objective to be accomplished. The next section includes the literature review and the key issues and challenges are discussed. Finally the paper includes a promising model which will enable us for supporting cloud security infrastructure.

II. LITERATURE REVIEW

This section involves the different techniques and methodologies that are supporting the proposed concept of securing information.

Smart grid is an innovation that improves efficiency, reliability, economics, and sustainability of electricity services. However, how to manage different types of front-end devices such as power assets and smart meters efficiently; and how to process a huge amount of data. Cloud computing is a technology that provides computational resources on demands. **J.Baek et al [1]** proposed a secure cloud based framework for big data management in smart grids,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 249-252 www.ijaem.net ISSN: 2395-5252

which call "Smart-Frame". The framework is to build a hierarchical structure of cloud datacenters to provide different computing services for information management and analysis. In addition, they present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues.

Table 1 review Summary

Reference	Domain	Methods	Outcome
[1]	Cloud based smart grid security	identity-based encryption, signature and proxy re-encryption	address critical security issues
[2]	secure data access for cloud computing platform	identity-based encryption and biometric authentication	An integrated data access scheme includes parameter setup, key distribution, feature template creation, data processing and secure data access control.
[3]	overhead at Private Key Generator (PKG) during user revocation	Identity-Based Encryption, hybrid private key	outsourcing computation into IBE, a revocable IBE scheme in the server-aided setting
[4]	Key exposure is one serious security problem	strong key-exposure resilient auditing for secure cloud storage	cloud storage auditing scheme with key-exposure resilience
[5]	Under open networks and not fully trusted cloud environments, thus we face security and privacy riskswhen outsourcing their data to a public cloud	Review	dwell on existing solutions to achieve secure, dependable, and privacy-assured cloud data services including search, computation, sharing, storage, and access
[6]	challenge associated with existing designs is the complexity in key management	introducing fuzzy identity-based auditing	formalize the system model and the security model, develop a prototype implementation of the protocol

Cloud computing consists of many large datacenters which are usually geographically distributed. How to design a secure data access for cloud computing platform is a big challenge. **Cheng Hongbing et al [2]** propose a secure data access scheme based on identity-based encryption and biometric authentication. First, describe the security concern and then propose an integrated data access scheme, the procedure of the proposed scheme include parameter setup, key distribution, feature template creation, data processing and secure data access control. Finally, compare the scheme with other schemes through simulation. The results show that the data access scheme is feasible and secure.

Identity-Based Encryption (IBE) simplifies the public key and certificate management at Public Key Infrastructure (PKI) to public key encryption. However, one of the main drawbacks of IBE is the overhead at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the management of certificates is precisely the burden. **Jin Li et al [3],** aiming at tackling the critical issue of identity revocation, they introduce outsourcing computation into IBE and propose a revocable IBE scheme in the server-aided setting. The scheme offloads most of the key generation operations during key-issuing and key-update processes. This goal is achieved by utilizing a novel collusion-resistant technique: employ a hybrid private key for each user, in which an AND gate is involved and bound the identity component and time. They also formulized Refereed Delegation of Computation model. Finally, provide results to demonstrate the efficiency.

Key exposure is one serious security problem. In order to deal with, cloud storage auditing

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 249-252 www.ijaem.net ISSN: 2395-5252

scheme with key-exposure resilience has been proposed by **Jia Yu et al [4]**. In such a scheme, the malicious cloud might still or forge valid authenticators than it obtains the secret key of data owner. Authors propose strong key-exposure resilient auditing for secure cloud storage, in which the security auditing not only earlier, but also later than the key exposure. They formalize the definition and the model of cloud storage auditing and design. The key exposure in one time period doesn't affect the security storage auditing. The security proof and the results demonstrate that proposed scheme achieves desirable security and efficiency.

Under open networks and not fully trusted cloud environments, thus we face security and privacy riskswhen outsourcing their data to a public cloud. To fully understand the advances and discover the research trends, this survey summarizes and the state-of-the-art technologies. **J. Tang et al [5]** first present security threats and requirements of an outsourcing data to a cloud, and follow overview of the security technologies. Then dwell on existing solutions to achieve secure, dependable, and privacy-assured cloud data services including search, computation, sharing, storage, and access. Finally, proposed open challenges and directions in each category.

A core security issue in cloud storage is data integrity. Data auditing protocols enable to efficiently check the integrity of the data without downloading. A key research challenge associated with existing designs is the complexity in key management. **Y. Li et al [6]** address complex key management challenge in cloud data integrity checking by introducing fuzzy identity-based auditing. Specifically, present the primitive of fuzzy identity-based data auditing, where a user's identity can be viewed as a set of attributes. They formalize the system model and the security model,and then present a fuzzy identity-based auditing protocol by utilizing biometrics as the identity. The protocol offers the property of error-tolerance, namely, it binds private key to one identity which can be used to verify the correctness of a response generated with another identity, if and only if both identities are close. They prove the security based on the Diffie-Hellman assumption and the discrete logarithm assumption. Finally, develop a prototype implementation of the protocol.

III. PROPOSED WORK

The previous section demonstrates the different research efforts in the direction of securing the cloud data storage.The key issue in cloud data storage is the security challenges and data integrity during outsourcingof data. In this context we found a noteworthy contribution which motivated us to study about the cloud storage security and validity check [7]. In this presented work the security model is described that usages the identity of data owner and provides integrity check for the communicated data between client and server. That technique is sound and effective enough but needs the following technique to enhance the current security process.

1. The given methodology have a higher computational complexity and communication cost
2. Requires a secure mechanism for key exchange
3. The third party is assumed as the completely trusted

In order to enhance the model in this study we propose a cloud data storage and validity check infrastructure using cryptographic technique. The basic model architecture is demonstrated in figure 1. .

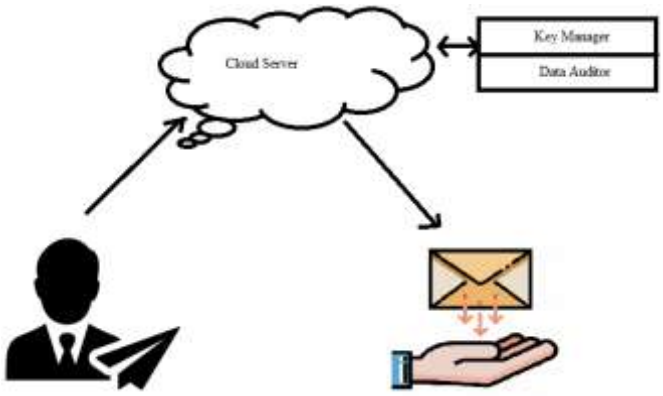

Figure 1 proposed system architecture

1.
Third party is not assumed to be completely trusted
2. No key is exchanged among any party

3. Only the integrity information is shared during communication remaining parameters are used only one time for security

Moreover the technique is more enhanced by using identity based cryptography. Those technique usages the two major concepts to enhance the security first involvement of third party authority that not knows about client and the communicated data. Secondly the key generation is performed on the basis of data which is not disclosed at any point of communication. In additionally for securing the key and other communication random manner of data communication is performed.

VI.CONCLUSIONS

The security is a primary need when the data is travelling through the un-trusted network. A number of confidential and private information is transferred through the network. The security during communication is a key challenge even if the data is preserved on cloud. In this presented work a cloud security model is presented that not only used to secure the data during transmission, which also provide an Integrity check using the remote server. In addition of that it is also promises to provide the original data to their actual users who are the data owners. Therefore an access control policy is also implemented with the proposed cryptographic concept. The current study provides the literature survey about the proposed concept and an overview of the proposed solution.

REFERENCES

[1] J.Baek, Q.Hieu Vu, J. K. Liu, X. Huang, Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", 7th IEEE International Conference for Internet Technology and Secured Transactions, London, UK, December 2012

[2] C.Hongbing, R.Chunming, T.Zhenghua Z.Qingkai, "Identity Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing", Chinese Journal of Electronics Vol.21, No.2, Apr. 2012

[3] J. Li, J. Li, X. Chen, C.Jia, W. Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing", IEEE Transactions on Computers Vol: 64 No: 2 Year 2015

[4] J. Yu, H. Wang, "Strong Key-Exposure Resilient Auditing for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, 2016

[5] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, R.Buyya, "Ensuring Security and Privacy Preservation for Cloud Data Services", ACM Comput. Surv. 49, 1, Article 13 (June 2016), 39 pages, DOI: http://dx.doi.org/10.1145/2906153

[6] Y. Li, Y. Yu, G. Min, W.Susilo, J. Ni, K. K. R. Choo, "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems", Journal of Latex Class Files, Vol. 14, No. 8, August 2015

[7] Y. Yu, M. H. Au, G.Ateniese, X. Huang, W.Susilo, Y. Dai, G. Min, "Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information Forensics and Security, 12 (4), 767-778, 2016.