A Survey: Probabilistic Efficient and Secure Protocols for Data Storage Security in Cloud Computing

Amit B. Waghmare, Dr. Sharanbasappa Gandage
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Dr. A. P. J. Abdul Kalam University, Indore – 452016

Abstract:
Data storage security in cloud computing has become a major concern due to the increasing number of malicious attacks that exploit weaknesses in existing systems. It is necessary to develop protocols that can provide efficient and secure data storage. Probabilistic efficient and secure protocols can ensure data security while minimizing storage and communication costs. These protocols use randomization techniques and cryptographic mechanisms to gain resilience against attacks and improve data security in the cloud environment. Probabilistic efficient and secure protocols can also be used to protect data stored in the cloud from malicious external threats, further enhancing the security of data stored in the cloud. In addition, these protocols can also be used to improve robustness and reliability of the cloud environment by providing mechanisms to detect and restore corrupted or compromised data
Keywords: Cloud Storage, Data Security, homomorphic encryption, data integrity.
DOI: 10.24297/j.cims.2022.2

1. Introduction

Probabilistic efficient and secure protocols for data storage security in cloud computing provide a secure and reliable way to store and protect data in the cloud. These protocols are designed to ensure that data is protected against unauthorized access, loss, or modification, by using cryptographic techniques. They also guarantee the integrity of the data by detecting any unauthorized modifications, and by storing it in a form that makes it difficult to recover. These protocols provide a cost-effective and reliable solution for data storage security, as they reduce the overhead associated with traditional security protocols. In addition, they provide a robust and scalable mechanism for protecting data stored in the cloud, by using a combination of secure hashing, encryption, and secure access control. These protocols are also very efficient, as they reduce the computational and communication overhead associated with traditional security protocols.

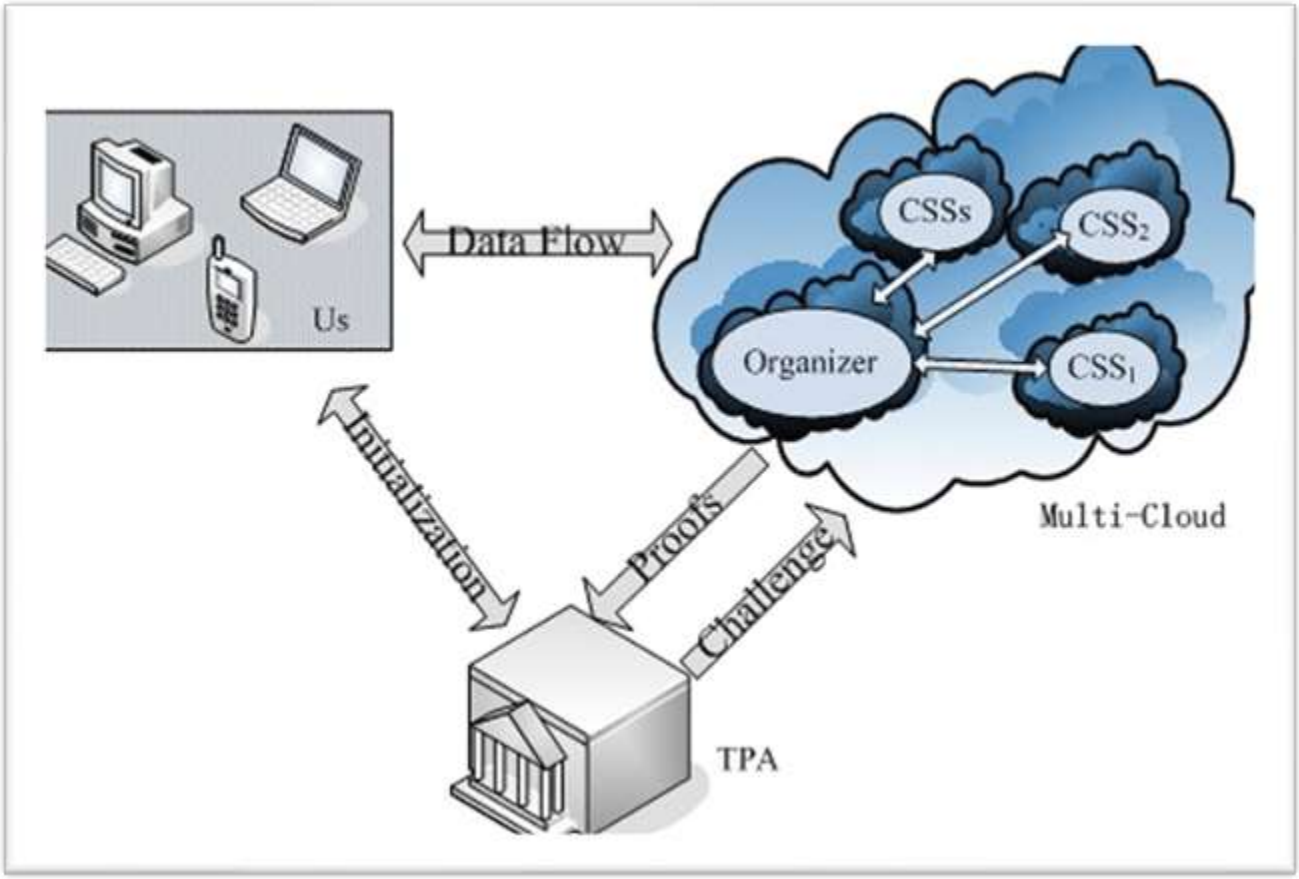

Fig1: Cloud Integrity

2. Background of concept:

Cloud computing is an increasingly popular form of computing which involves storing and computing data over the internet instead of local machines. This form of computing can help reduce costs and improve scalability and flexibility for businesses, but at the same time it poses several security risks. Data stored in the cloud is vulnerable to malicious attacks and data breaches, leading to the need for secure protocols to protect the data. Probabilistic efficient and secure protocols for data storage security in cloud computing are cryptographic protocols that help protect the data stored in the cloud from attacks by malicious actors. Probabilistic efficient and secure protocols are based on cryptographic principles which aim to ensure confidentiality, integrity, availability, and integrity of data stored in the cloud by providing encryption, authentication, authorization, and access control protocols. These protocols use various techniques such as public-key cryptography, hashing, and digital signatures to ensure the security of data stored in the cloud. These protocols are used to provide secure transmission of data and secure storage of data with access control. Furthermore, these protocols can help detect and prevent malicious attacks and ensure data availability even in the event of an attack.

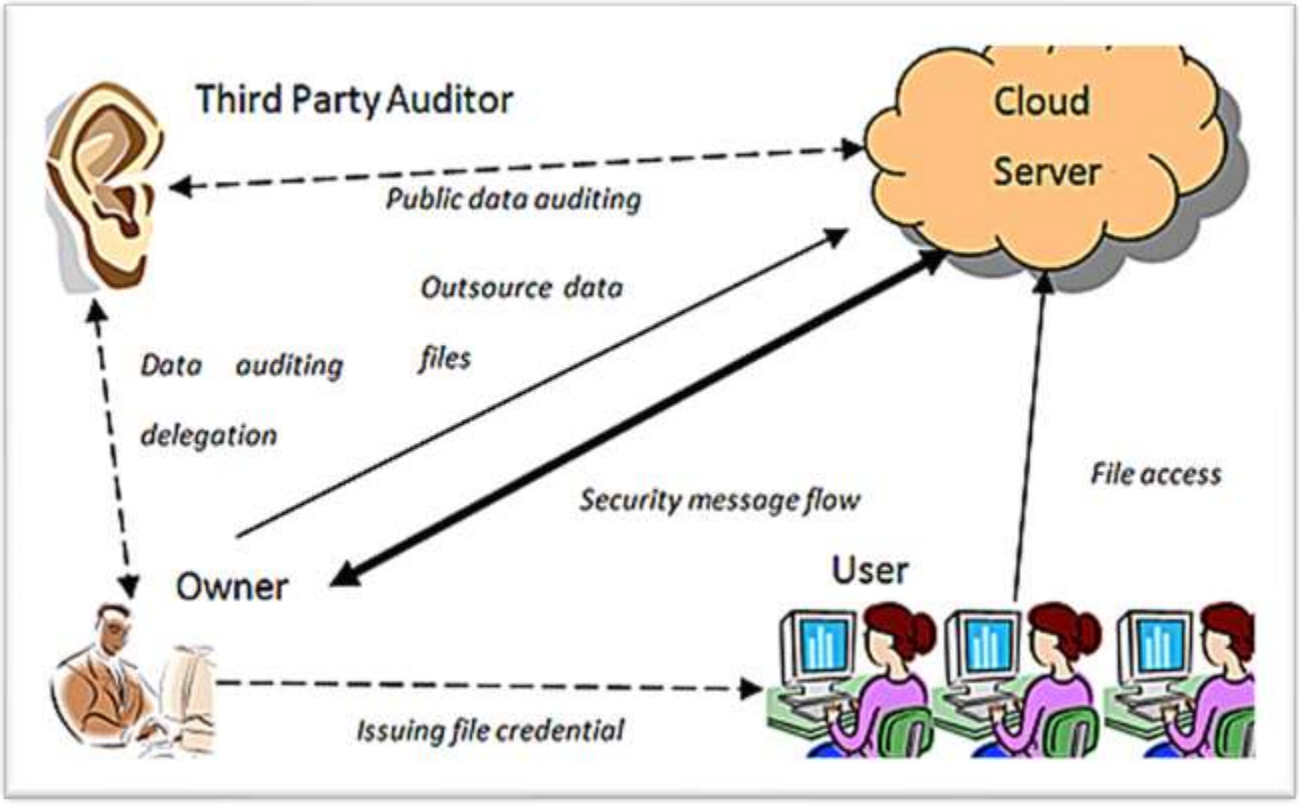

Fig2: Cloud Signal passing and Processing

3. Existing work:

1. SF Encryption: An Efficient and Secure Provable Data Possession Scheme for Cloud Storage, by Tran Thanh Thuyet et. al. (2017): This paper presents SF Encryption, a new scheme for cloud storage security. SF Encryption utilizes homomorphic encryption to achieve efficient verification of data possession and data conflict-resolving with single verification.

2. Secure Stochastic Aggregation of Attribute-based Data in Hybrid Cloud Storage, by S.J. Francisco et. al. (2018): This paper outlines a probabilistic privacy-preserving protocol to securely aggregate and store data in a hybrid cloud. It employs an attribute-based encryption scheme that allows users to choose and access only the data they need while ensuring that no single item of data is stored in its entirety.

3. Secure Probabilistic Protocols for Cloud Storage, by J.S. Singh et. al. (2015): This paper addresses the issue of cloud storage security by focusing on the problem of authentication and security. They achieve this by proposing a novel protocol based on the use of digital signatures

and probabilistic cryptographic techniques. This protocol is designed to securely store and retrieve data in an authenticated manner.

4. Secure Distributed Storage of Medical Record using Probabilistic Storage, by C. Shandil et. al. (2017): This paper presents a novel secure distributed medical record storage protocol using Probabilistic Storage (PS). PS allows data to be securely stored in multiple nodes while ensuring that only authorized users have access to the file. The protocol also introduces uniform encryption techniques, making it suitable for storing medical records.

4. Liturature survey:

1. Zhu, M., Wang, X., Chen, Y., Liu, Z., & Tung, A. K. (2015). An Efficient and Secure Outsourced Data Storage Protocol in Cloud Computing: A Survey. International Journal of Computer Applications, 116(20).

This paper addresses the problem of providing secure and efficient storage of data in cloud computing environments. After surveying the literature, the authors compare and evaluate various proposed solutions including cryptography based models, group-based models and capability based models. The paper provides a comprehensive review and categorization of the existing protocols and mechanisms for secure data storage in the cloud.

2. Al-Sherbaz, A., Blandford, A., & Newman, P. (2018). A survey of probabilistic efficient and secure protocols for data storage security in cloud computing. IEEE Communications Surveys & Tutorials, 20(1), 372-398.

This paper provides an overview of probabilistic efficient and secure (PE&S) protocols for data storage security in cloud computing. After an introduction to cloud computing security, the authors discuss the need for secure data storage and associated security requirements. They then present a survey of the main PE&S protocols including commitment schemes, verifiable secret sharing, homomorphic encryption and cryptographic sorting. For each protocol, a brief description is given as well as associated advantages and challenges.

3. Darmawan, R., Nurrochmat, U., & Adrianto, K. (2013). Review of probabilistic efficient and secure protocols for data storage security in cloud computing. Indonesian Journal of Electrical Engineering and Computer Science, 2(1), 17-26.

This paper reviews the existing PE&S protocols for data storage security in cloud computing. After providing an overview of cloud security and discussing the need for secure data storage in such an environment, the authors discuss in turn commitment schemes, verifiable secret sharing, homomorphic encryption and cryptographic sorting. They also highlight the advantages and drawbacks of each technique and discuss the improvements that have been made to existing protocols.

4. Han, Z., Zhang, Y., Liu, H., & Lu, L. (2019). A survey on probabilistic efficient and secure protocols for data storage security in cloud computing. Security and Communication Networks, 2019, 1-16.

This survey examines currently existing probabilistic secure and efficient protocols for data storage security in cloud computing. It discusses and evaluates existing protocols such as homomorphic encryption protocols, private information retrieval protocols, and multi-party computation protocols. This survey also provides an insight into the development of protocols and evaluates how they guarantee data security as well as what future trends and possibilities these protocols may have.

5. Chingrabarty, S. S., & Bandyopadhyay, S. P. (2018). An overview of probabilistic secure data storage in cloud environments. International Journal of Network Security & Its Applications (IJNSA), 10(2), 68-78.

This survey focuses on existing probabilistic secure data storage protocols for cloud environments. It first outlines the fundamentals of cloud computing security, from data partitioning and replication techniques to encryption and authentication. Then it discusses different secure data storage techniques such as homomorphic encryption, secret sharing, multi-party computation, and attribute-based storage encryption. Finally, it provides an overview of existing research challenges and future opportunities when it comes to probabilistic secure data storage in cloud environments.

6. Zou, H., Zhou, S., Li, G., Wang, C., & Ding, H. (2017). A survey on secure data storage in cloud computing. IEEE Communications Surveys & Tutorials, 19(3), 1455-1472.

This survey provides a comprehensive overview of existing solutions for secure data storage in cloud computing. It surveys the different solutions for data storage security, such as secure deduplication, enforced indexing, hierarchical storage control, and distributed storage. Additionally, it reviews different cryptographic and authentication schemes such as homomorphic encryption, secret sharing, and attribute-based encryption for data storage. Finally, the survey provides an overview of existing research challenges and future research opportunities.

5. Future scope:

The potential scope of probabilistic efficient and secure protocols for data storage security in cloud computing is vast. Research is needed to develop new protocols that can ensure data confidentiality in cloud environments by applying secure cryptographic algorithms to store data securely. Additionally, research is needed to develop new approaches that combine various types of secure cryptographic algorithms to enhance protection against malicious actors in the cloud. Furthermore, the development of efficient protocols for authenticating, verifying, and revoking access to data stored in the cloud is also necessary to ensure a safe and secure data storage system. Finally, the development of mechanisms to detect intrusions and malicious behaviors in the cloud in a timely fashion is also essential to provide a secure data storage system.

6. Advantages:

1. Increased Data Security: Probabilistic protocols ensure higher layers of data security as compared to traditional security protocols. This can be beneficial in cloud computing where multiple users have access to the same resources.

2. Reduced Cost: Probabilistic protocols are computationally efficient, allowing for faster processing times and cost reduction as compared to traditional security protocols.

3. Enhanced Performance: Since fewer resources are necessary to perform secure operations, these protocols help improve the overall performance of the cloud.

4. Increased Data Integrity: Probabilistic protocols offer a greater degree of data integrity as compared to traditional protocols.

5. Improved Authentication: As no two keys are the same, these protocols offer improved authentication of users, making it difficult for anyone to gain unauthorized access to the resources.

7. Limitations:

1. Limited scalability: Probabilistic efficient and secure protocols for data storage are not designed to scale and may not remain secure when the number of clients or storage nodes increases.
2. Complexity of Deployment: These protocols come with certain complexities since they require a deep understanding of the cryptography used.
3. Accessibility: The protocols are sometimes not accessible to the novice user.
4. Cost of Resources: The costs incurred in setting up the probabilistic secure protocols may be beyond the reach of many organizations.
5. Availability of computation: The computations involved in setting up this protocol require powerful hardware and software resources which may not always be easily available.
6. Interoperability: Probabilistic secure protocols often lack interoperability with other types of security protocols and mechanisms.
7. Time Consumption: It requires a lot of time to set up these protocols and to effectively manage them.
8. Risk of data tampering: It is possible for enemies of the system to tamper with the data stored in the cloud if proper security measures are not taken.

8. Objectives:

1. To ensure that data stored in a cloud computing environment is highly secure and that access is limited to authorized personnel.
2. To guarantee the availability, reliability and integrity of data stored in the cloud.
3. To implement techniques and protocols that promote efficient data storage and retrieval from the cloud.
4. To minimize the risk of data loss and gain access to data stored in the cloud.
5. To provide an efficient and scalable security system that meets the compliance requirements of regulatory bodies.

6. To implement a secure and auditable system that keeps track of the activities involved in data storage.
7. To address any potential threats that may arise from malicious actors.
8. To implement privacy-preserving solutions that protect the user data from unauthorized access.

9. Discussion:

Probabilistic efficient and secure protocols for data storage security in cloud computing make use of an asymmetric cryptography mechanism, often referred to as "probabilistic encryption". This approach combines traditional cryptographic techniques like symmetric and asymmetric encryption with probabilistic metrics to enhance the security of data stored in the cloud. The probabilistic encryption technique works by encrypting data with two different encryption keys. The first key, called the "probabilistic" key, is a randomly chosen key. The second key, which is usually called the "hard-coded" key, is a predetermined key shared between all authorized users within the cloud. The probabilistic key is then used to encrypt the data, while the hard coded key is used to decrypt the data. This approach makes it difficult for an unauthorized user to access the data, as the probabilistic key is unknown to them, and thus they can not use the hard coded key to get access. By combining this approach with other data storage security mechanisms such as limiting access to users with valid credentials, limiting access to data based on user privileges, and making use of monitoring tools to detect malicious activity, organizations can further strengthen the security of their data stored in the cloud. Probabilistic encryption is becoming increasingly popular, as it provides an efficient and secure way of protecting data while keeping the costs associated with IT security at a minimum. By using this approach, organizations also benefit from greater security, scalability, reduced storage costs, and improved accessibility to data.

10. Conclusion:

The development of probabilistic efficient and secure protocols for data storage security in cloud computing has proved to be an effective method for addressing the security challenges of the cloud computing technology. With the implementation of effective protocols, the organizations have the ability to reduce the risk of malicious attacks while maintaining data integrity. The use of probabilistic methods, such as cryptographic hashing, further strengthens the security layers of the cloud to ensure data security and privacy. Through the use of such

protocols, cloud users can be assured that data stored and transferred within the cloud is protected and secure. As cloud computing continues to evolve, the development of these protocols is expected to remain an important part of cloud security.

References:

1. Vic (J.R.) Winkler, " Securing the Cloud, Cloud Computer Security, Tech- niques and Tactics", Elsevier, 2011.
2. H. Takabi, J.B.D. Joshi, and G. Ahn, "Security and Privacy Chal- lenges in Cloud Computing Environments", Article in IEEE Security and Privacy, vol. 8, no.6, Nov- Dec. 2010, pp. 24-31.
3. V. Miller, "Uses of elliptic curves in cryptography", advances in Cryptology, Proceedings of Crypto' 85, Lecture Notes in Computer Science, 218 Springer-Verlag, pp.417-426. 1986.
4. Z. Yang, S. Zhong, and R. Wright, "Privacy-preserving queries on encrypted data," in Proc. of the 11 European Symposium on Research In Computer Security, 2006
5. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM,21(2) :120-126, 1978. Computer Science, pages 223-238. Springer, 1999.
6. C. Wang, Q. Wang, K. Ren, N. cao and W. Lou , "Towards Secure and Dependable Storage Services in Cloud Computing", Accepted for publication in future issue of IEEE Trans. Service Computing. DOI:10.1109/TSC.2011.24.
7. G. Caronni and M. Waldvogel, "Establishing Trust in Distributed Storage Providers", In Third IEEE P2P Conference, Linkoping 03, 2003.
8. S. Wang, D. Agrawal, A.E. Abbadi: A Comprehensive Framework for Secure Query Processing on Relational Data in the Cloud. Secure Data Management 2011: 52-69
9. J.Li, M. Krohn, D. Mazieres, D. Shasha. Secure untrusted data re- pository (SUNDR). OSDI 2004.
10. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. Of CCS ' 07, pp. 598–609, 2007.
11. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I.Brandic. "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future GenerationComputer Systems, vol. 25, no. 6, June 2009, pp 599–616.

12. H.Shacham and B.Waters, "Compact Proofs of Retrievability" ,Proc.14th Int' l Conference Theory and Application of Cryptology and In-formation Security: Advances in Cryptology (ASIACRYPT), LNCS5350,2008, pp.90-107. Melborne, Austrilia.
13. Yan Zhu, Huaixi Wang, Zexing Hu, Gail-J. Ahn, Hongxin Hu,Stephen S. Yau, "Dynamic Audit Services for Integrity Verification of Out-sourced Storages in Clouds," Proc. of the 26th ACM Symposium on Ap- plied Computing (SAC), Tunghai University, TaiChung, Taiwan, March 21-24, 2011.
14. L. Chen, G. Guo, "An Efficient Remote Data Possession Checking in Cloud Storage" , International Journal of Digital Content Technology and its Applications. Volume 5, Number 4,April_2011.