Journal of
Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766319

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
Corresponding Author: amitw63@gmail.com

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

INTRODUCTION:

Cloud computing is a rapidly growing technology that enables users to access and store data in online servers, or 'the cloud'. Despite its convenience, data stored in the cloud can be vulnerable to different kinds of attacks and privacy violations. To ensure data security, a secure protocol can be used to provide the necessary cryptography, authentication, and data signing. This protocol defines specific rules, processes, and mechanisms for data storage and retrieval that guarantees secure transmission and storage of data. It incorporates advanced encryption mechanisms to ensure secure transmission and storage of data, and data access control to ensure only authorized entities have access to the data. Additionally, the security protocol may also provide for digital signature algorithms to protect the integrity of the data, and periodic audit of data to detect tampering or data corruption.

By implementing a secure storage protocol, organizations can benefit from increased data security, privacy, and authentication. Furthermore, organizations can reduce the risk of data leakage and unauthorized access through encrypting sensitive data. Moreover, using a secure protocol can improve the reliability of cloud services, while providing a heightened layer of trust to users. With encrypted data and improved security protocols, users can be sure that their data remains protected in the cloud.

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.

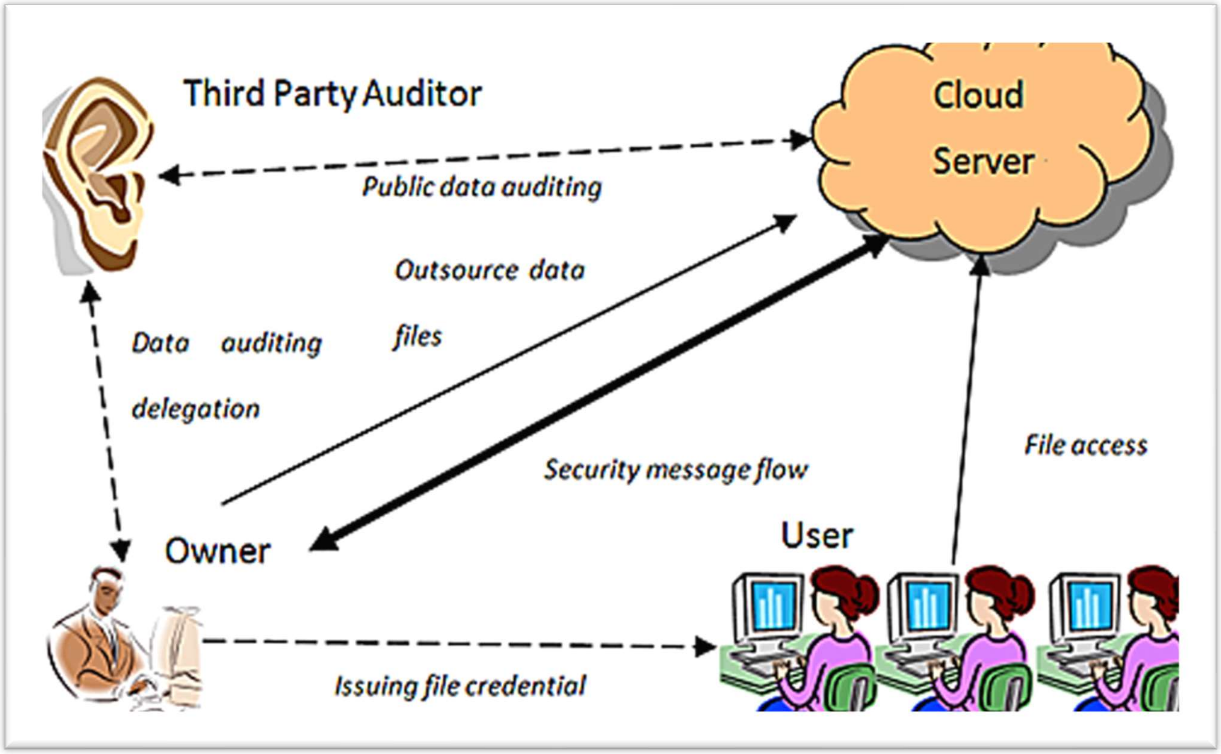

Fig2: Cloud Signal passing and Processing

Study of Some secure protocols:

- SSL/TLS) / SSH SSL/TLS:

(Secure Sockets Layer/Transport Layer Security) is an encrypted communications protocol used to secure communication between two Internet-connected parties. It is used to secure communications between web browsers and web servers, secure email, VPNs, secure financial transactions, chat networks, and more. SSH (Secure Shell) is a cryptographic network protocol for securing remote shell sessions between two computers. It provides secure access to a remote system, secure file transfers, remote command execution, and other network-level services over an unsecured network. SSH is used for secure remote login, remote system administration, and secure file transfer.

- *IPsec*

(also referred to as Point-to-Point Tunneling Protocol or PPTP) is a secure, encrypted connection between two networks or two Computers over the public internet. IPsec provides authentication, integrity and confidentiality. It is commonly used for creating Virtual Private Networks (VPNs) that allow people to access networks from remote locations securely.

- *Kerberos*

A Kerberos ticket granting ticket (TGT) is an authentication token used in the Kerberos authentication system. It is issued by a Key Distribution Center (KDC) to a Kerberos user when they successfully authenticate, and which is used to request service tickets. The TGT consists of a session key and some identity information, encrypted in the KDC's secret key. The user presents the TGT to the KDC each time they need to request a service ticket, so the KDC can verify their identity without requiring additional authentication.

- *S/MIME*

Its works in EMail, Storage PGP EMail, Storage, Instant Messaging Pretty Good Privacy EMail, Storage, Instant Messaging

- *Pretty Good Privacy (PGP)*

Pretty Good Privacy (PGP) is a data encryption program that provides cryptographic privacy and authentication for online communication. It is used to encrypt email, text messages, and other files to ensure that the contents of the communication are secure and kept private. PGP uses asymmetric encryption, which is a form of encryption where two different keys are used to encode and decode a message. The public key is used to encrypt the message, while the private key is used to decrypt it. PGP also includes an authentication process, which ensures that the sender is who they claim to be. This is achieved by a type of digital signature created with the sender's private key. The sender's public key is used to verify the signature. PGP is popular among individuals and companies looking to ensure the security of their confidential information. It is also popular with privacy and digital rights advocates who want to protect their data from surveillance and other intrusions.

- *AES Encryption*

AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm used for data encryption. It is a form of encryption that has been adopted by the US government and is used worldwide for secure data transmission. AES uses a key of 128, 192, or 256 bits, which is then used to encrypt data using either the Electronic Codebook (ECB), Cipher Block Chaining (CBC), or Counter Mode (CTR) modes. The key is then combined with an initialization vector (IV) to create an encryption key for the data. The key length determines the level of security of the encryption, with a longer key providing a higher level of security. AES is considered to be a very secure form of encryption, and is widely used for encrypting data, such as credit card numbers, passwords, and other sensitive information.

- *HIPAA*

HIPAA is the Health Insurance Portability and Accountability Act of 1996. It is a federal law that requires healthcare organizations to keep individuals' medical records and other health information private and secure. The act also requires organizations to provide notification about the use and disclosure of protected health information (PHI). The law also requires organizations to have certain measures in place to ensure the privacy and security of PHI, such as the use of encryption and other technical safeguards.

- *Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. ECC requires the use of a public or private key system. In a public key system, users must keep their private keys secure and accessible only to them. The private key is used to decode messages that were encrypted using a public key. In order for a public key system to work, users must distribute their public keys to other parties they want to communicate with. The security of ECC relies on the difficulty of solving for discrete logarithms on the points of an elliptic curve. Discrete logarithms are derived from mathematical equations and the difficulty of solving them increases exponentially with the size of the key. This makes ECC secure and virtually unbreakable. As an additional benefit, ECC is computationally efficient which makes it ideal for mobile and embedded systems. The large key sizes that are often required for non-ECC systems can cause data and computation overload. ECC's smaller keys and faster algorithms make it fast enough for use on low-powered devices.

- *Identity-Based Encryption (IBE)*

Identity-based encryption (IBE) is an encryption technique that uses the identity of the user as a public key to encrypt confidential data. IBE provides a solution to the problem of distributing certificates and ensures the confidentiality of messages without the need for public-key infrastructure. IBE works by generating shared public/private keys based on the identity of users, which is certified by a private, trusted entity such as a certification authority. Public keys are generated and signed by the trusted entity, while private keys are generated by the user. When a user needs to send a message, they encrypt the message with the recipient's public key and the recipient can decrypt the message with their corresponding private key. IBE is an emerging encryption technology that is gaining popularity due to its use of identities as public keys which simplifies key management. It is ideal for applications such as smart cards, which require strong encryption but need to maintain identities of users.

- *Secure Multipurpose Internet Mail Extensions (S/MIME)*

S/MIME is a security protocol used to allow secure transfer of email and other data over the internet. It works by using certificates and encrypted messages, which ensures that messages are secure and tamper-proof between sender and receiver. It is most commonly used in organizations such as governments, corporations, and universities to protect their communication. S/MIME's strong authentication, encryption, and message integrity capabilities provide a secure communications channel that can be used to protect sensitive information from malicious parties. Additionally, S/MIME provides beneficial features such as digital signatures, email timestamping, and secure storage of outgoing emails. These features make it an ideal security solution for secure communication between business partners.

- *FIPS 140-2*

FIPS 140-2 certification The U.S. federal government requires the use of the FIPS 140-2 standard for cryptographic modules used in certain secure applications. FIPS (Federal

Information Processing Standard) 140-2 is an information assurance standard developed by the National Institute of Standards and Technology (NIST). It is based on requirements from the Department of Commerce, and outlines approved ways to use cryptographic algorithms. Both vendors and end-users must prove that products meet this standard to receive certification. Vendors must submit their products to an accredited third-party laboratory that tests the device for FIPS 140-2 compliance. Once certified, the product will have a Cryptographic Module Validation Program (CMVP) number, which can be validated on the NIST website.

- *Public key cryptography*

Public key cryptography, also known as asymmetric key cryptography, is a type of cryptography that uses two mathematically-related, but different, cryptographic keys—a public key and a private key—in order to encrypt and decrypt data. The public key can be given to anyone who wants to send the user data, while the private key must remain secret to the user so they can decode any messages sent to them using the public key. This type of cryptography is used frequently to securely send data over the internet using encryption protocols such as SSL/TLS.

- *Certificate-based authentication*

Certificate-based authentication is a type of authentication used to verify that a user requesting access to a system is who they say they are. It involves the use of a digital certificate, which is a digital document that binds the identity of a user or a computer to a public key. The certificate is issued by an authoritative third party, such as a certificate authority (CA) or domain controller. It uses public key cryptography, which requires two keys – one that the user has to prove ownership and one that the verifier has to decode the message. Certificate-based authentication helps protect against spoofing, because it requires the verifier to demonstrate that it knows the certificate-holder's identity and can access the certificate carrier's authorized key. It also prevents man-in-the-middle attacks, as the two sides must be in possession of the same secret key to encrypt and decrypt the message.

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.

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.

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.

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.

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 Outsourced 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.