JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE CLOUD STORAGE DATA INTEGRATION AUDITING WITHOUT PRIVATE KEY STORAGE

Devabattula Sudha Kala[1], M.Radhika Mani[2], A.Harini[3]
[1]**PG Student,** Dept of CSE, Pragati Engineering College (Autonomous), Surempalem,AP
[2]**Professor,** Dept of CSE, Pragati Engineering College (Autonomous), Surempalem,AP
[3]**AssistantProfessor,** Dept of CSE, Pragati Engineering College (Autonomous), Surempalem,AP
Email: sudhakala98@gmail.com[1], drradhikamani@gmail.com[2], harini.a@pragati.ac.in[3]

Abstract
Customers may store their data in the cloud utilising distributed storage administrations to minimise the requirement for local storage and maintenance resources. So far, several different methods for checking the integrity of cloud-stored information have been proposed. Clients are now obliged to utilise their private keys to produce information authenticators, which are used to evaluate the data's trustworthiness. So, in order to keep his private key, the customer must have a token (such as a USB token or a shrewd card) and memorise a secret word. Assuming the equipment token or the secret key are lost or ignored, several existing information integrity evaluation approaches would be rendered ineffective. Instead of holding private keys indefinitely, we suggest a new notion called information respectability review. In place of the equipment token, a biometric private key (such as an iris scan or a unique fingerprint impression) is utilised to safeguard the equipment for the end-user. As of present, the plan is capable of conducting data integrity tests. Direct sketching with code and error-correction cycles are two of the methods we use to verify the uniqueness of each client. Additional work is underway on a new mark design that maintains the trademark's blockless uniqueness while allowing it to be drawn by hand. The proof of security and the display analysis reveal that our suggested technique provides positive security and productivity.

Keywords: Cloud, Audit, Security, Private Key.

1. INTRODUCTION

Various cloud storage options are available to users [1]. As a result, customers no longer have to spend as much money on hardware maintenance in order to shift their data to the cloud. The private key might be stolen from the hardware token if it is compromised. If the user loses or forgets their hardware token, it is difficult to authenticate any new data block. Audits of data integrity will uncover a problem.

A strategy for doing data integrity audits without holding the secret key is thus both intriguing and tempting to researchers. Fingerprint and iris scan data may be used to produce the private key [2, 3]. Biometric data may be linked to a person's private key since it is part of the human body. Biometric data cannot be duplicated precisely due to a plethora of extrinsic factors. Because of factors such as pressure, wetness, presentation

angle, filth, and a variety of sensors, the fingerprint picture of each person is unique. Biometric data cannot be used as a private key for data integrity checks. Contribution This investigation's key conclusions are as follows: We came up with a new way to verify data integrity without storing a private key in our early research on biometric data as a fuzzy private key. The biometric data of a user is used to produce fudged private keys. If the private key is not stored on a hardware token, data integrity checks are available. Improved is the concept of data integrity auditing with no requirement for private keys to be stored in the secure cloud. Since private key information is no longer required for safe cloud storage, a realistic data integrity auditing system has been developed. Two biometric private keys (fuzzy private keys) are extracted from a user during registration and signature creation. Drawings with coding and mistake correction procedures are created using these two fuzzy private keys. A user's identification is verified using two fuzzy private keys, which we compare to minimise "noise" from two images. Whether two sets of biometric data are sufficiently similar, it is feasible to determine if they were taken from the same individual. Other than that, they came from two different people. Without the storage of private keys, data integrity auditing presents a problem in constructing a signature that is both consistent with the linear sketch and less block verifiable. Fuzzy signatures are the foundation of a new signature method we've developed to address this problem, dubbed MBLSS. We do a security evaluation and provide performance justifications based on real-world examples. The results demonstrate the safety and efficacy of the suggested procedure.

2. PROPOSED SYSTEM

Data integrity auditing is possible without maintaining private keys for secure cloud storage in the system. At registration and signature creation, we extract two biometric private keys (fuzzy private keys). Both of our fuzzy private keys were used to construct a pair of line drawings that included coding and error correction procedures. By decreasing the "noise" in a pair of drawings, we can validate the identity of the user. It's possible to tell whether the two sets of biometric data were acquired from the same individual by comparing them to one another. Blockless verifiability implementation is hampered by the fact that private keys cannot be stored in a secure location. We came up with a new signature scheme called MBLSS based on the concept of fuzzy signatures in order to address this issue. Based on real-world implementations, we give security analyses and performance explanations. Results show that the suggested method is safe and effective, according to the study.

3. ALGORITHM

A fuzzy signature scheme which is associated with a fuzzy key setting FKS = ((d, Y), γ, ε, Ω, θ) includes the following four algorithms:

a) Setup: The fuzzy key setting description FKS and a security parameter k are entered into the setup procedure (k defines the threshold value ε of FKS), and a public parameter pp is generated.

b) KeyGen: The public parameter pp and biometric data are inputs to the algorithm that generates the key $y \in Y$, verifies the key and produces a new one vk.

c) SigGen: Biometric data and a public parameter pp are used as inputs to the signature creation method. y 0 ∈ Y and a data block mi , and generates the signature σi of mi

d) Verify: The method requires a public parameter pp, a verification key vk, a data block mi, and the signature as input σi of mi , and returns 1 or 0 to prove the signature σi is valid or not.

4. PROPOSED SYSTEM ARCHITECTURE

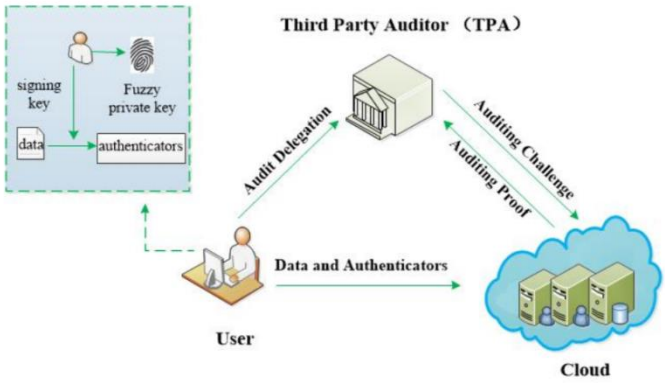

Fig1: Proposed Architecture

The system model shown in Fig. 1 consists of users, clouds, and TPAs. The cloud has a lot of storage space accessible for customers to store their data in. There are a lot of files that need to be uploaded to the cloud by the end user. TPAs are public verifiers that are entrusted with assuring the integrity of data that is stored in a cloud service.

During the registration procedure for the cloud storage service, the user's biometric data (such as a fingerprint) is collected. A biometric key generated from previously acquired data is used to generate a random signing key before data is uploaded to the cloud for safekeeping and access by authorised users. The owner of the data then generates data block authenticators using his signing key. They are uploaded to the cloud and deleted from local storage after he completes this step. For data integrity audits, the TPA employs challenge-response protocols to verify that the cloud is protecting the integrity of its users' personal information.

5. EXPERIMENTAL RESULTS

It's possible for a user to access the operations of Cloud, TPA and Data Owner. It's possible to search for and download data The Upload File with Blocks, the View All Upload File with Blocks, the Data Integrity Audit, and the Transactions pages are all available to anyone who have access to the data. Actions may be retrieved on the cloud. Individuals can be seen and authorized. The file's owners may see and authenticate each and every block and transaction. The option to see all defendants is available. Access and Analyze Time Delay and Throughput Information.

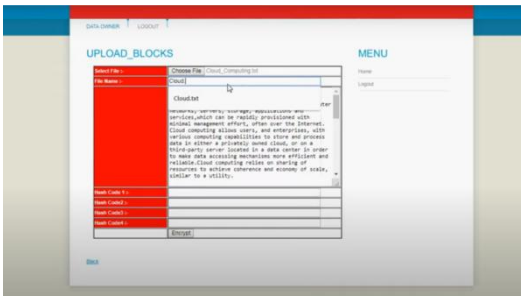

Fig5.1: Data Owner Upload Blocks

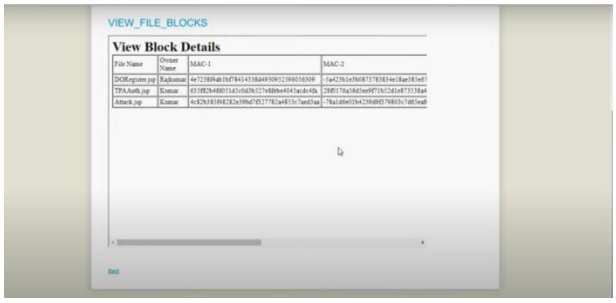

Fig5.2: Cloud View File Blocks

Fig5.3: Data User Download File

Fig5.4: View Results

6. COMPARATIVE STUDY

An allotted computing activity is to deal with capacity challenges of particular types, and moderate distributed computing merchants provide different storerooms to accommodate this need. Indeed, it is an enormous challenge to place oneself on such an enormous stage as that which scales with the World Wide Web. For the purpose of determining the requirements for these storage spaces, we appear to be in agreement with the capabilities provided by Amazon Web Services [4], Microsoft Windows Azure [5], and Google's AppEngine [6] thus as much in imitation of draw the potential requirements of large informational collections as like specific illustrations, then desire as it would run about so an in. Table 1 shows a variety of possible combinations offered by the three retailers.

Storage Type	Amazon Web Services	Windows Azure	Google AppEngine
Unstructured	Yes	Yes	Yes
Structured	Yes	Yes	Yes
Message Queue	Yes	Yes	Yes
Block Devices	Yes	Yes	No
RDBMS	Yes	Yes	No

Table 1: Comparative Study Storage Types

7. CONCLUSION

The use of a "fuzzy private key" means that integrity checks may be done without the need to store the private key. Data integrity assessments of cloud-based secure storage do not need access to private key information. It's possible to substitute the user's fuzzy private key with biometric data (such as fingerprint or retinal scan).

Signature verification and compatibility with linear drawings have also been included. Based on a thorough security and performance evaluation, we can confidently say that our suggested solution is both secure and efficient.

REFERENCES

[1] H. Dewan and R. C. Hansdah, "A survey of cloud storage facilities," in 2011 IEEE World Congress on Services,July 2011, pp. 224–231.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan 2004.

[3] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar 2003.

[4] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Identity-based remote data possession checking in public clouds," IET Information Security, vol. 8, no. 2, pp. 114–121, March 2014.

[5] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.

[6] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.

[7] B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," in International Conference on Applied Cryptography and Network Security, 2012, pp. 507–525.

[8] B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing for shared cloud data supporting group dynamics," in 2013 IEEE International Conference on Communications (ICC), June 2013, pp. 1946–1950.

[9] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.

[10] H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE Transactions on Cloud Computing, vol. 13, no. 9, pp. 1–14, 2014.

[11] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[12] N. Garg and S. Bawa, "Rits-mht: Relative indexed and time stamped merkle hash tree based data auditing protocol for cloud computing," Journal of Network & Computer Applications, vol. 84, pp. 1–13, 2017.

[13] H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.

[14] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacypreserving authenticators for cloud storage," Future Generation Computer Systems, vol. 76, no. Supplement C, pp. 136 – 145, 2017.

[15] C. Ellison and B. Schneier, “Ten risks of pki: What you’re not being told about public key infrastructure,” vol. 16, no. 1, 12 2000.

[16] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16,no. 1, pp. 69–73, Jan 2012.

[17] A. F. Barsoum and M. A. Hasan, “Provable multicopy dynamic data possession in cloud computing systems,”IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, March 2015.

[18] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in cryptology—EUROCRYPT 2005, ser. Lecture Notes in Comput. Sci. Springer, Berlin, 2005, vol. 3494, pp. 457–473.

[19] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp. 598–609.

[20] A. Juels and B. S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp. 584–597.

[21] H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[22] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” in ACM Symposium on Applied Computing, 2011, pp. 1550–1557.

[23] M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, “Dynamic remote data auditing for securing big data storage in cloud computing,” Information Sciences, vol.380, pp. 101–116, 2017.

[24] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for data storage security in cloud computing,” in 2010 Proceedings IEEE INFOCOM, March 2010, pp. 1–9.

[25] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, “Privacy-preserving public auditing protocol for low performance end devices in cloud,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, Nov 2016.

[26] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo,Y. Dai, and G. Min, “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017.

[27] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, “Symmetric-key based proofs of retrievability supporting public verification,” in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.

[28] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, “Opor: Enabling proof of retrievability in cloud computing with resource-constrained devices,” IEEE Transactions on Cloud Computing, vol. 3, no. 2, pp. 195–205, April 2015.

[29] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82,pp. 56–64, 2017.

[30] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302.