IJTRET

International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 4 August 2020
ISSN NO 2582-0958

DATA INTEGRITY AUDITING WITHOUT PRIVATE KEY STORAGE FOR SECURE CLOUD STORAGE

[1]R.Rajesh,[2] T.A.Vinayagam
[1]Student, [2]Associate Professor, Department of Computer Science & Engineering,
Sri Venkateswara College of Engineering and Technology,
Thiruvallur, Thirupachur, Tamil Nadu 631203

ABSTRACT

Utilizing distributed storage administrations, clients can store their Information in the cloud to maintain a strategic distance from the consumption of neighborhood information stockpiling support. To guarantee the uprightness of the information put away in the Cloud, numerous information, honesty examining plans have been proposed. A client needs to Utilize his private key to produce the information authenticators for Understanding the information respectability reviewing. In this way, the client needs to have an equipment token to store his private Key and retain a secret phrase to enact this private key. In the event that this Equipment token is lost or this secret phrase is overlooked, the majority of the Current information, trustworthiness inspecting plans would be notable work. We propose another worldview Called information uprightness inspecting without private key stockpiling and Plan such a plan. In this plan, we use biometric informationas the client's fluffy private key to Abstain from utilizing the equipment token. In the interim, the plan can at present Successfully complete the information respectability auditing. We use a direct Sketch with coding and blunder revision procedures to affirm The personality of the client. We use another mark Conspire which supports blacklist certainty. The security evidence and the Execution examination demonstrates that our proposed plan accomplishes Attractive security andeffectiveness.

Keywords: *Cloud storage, Data integrity auditing, Data security, Biometric data*.

1.INTRODUCTION

Cloud storage can provide powerful and on-demand data storage services for users. By using the cloud service, users can outsource their data to the cloud without wasting substantial maintenance expenditure of hardware and software, which brings great benefits to users. However, once the users upload their data to the cloud, they will lose the physical control of their data since they no longer keep their data in local. Thus, the integrity of the cloud data is hard to be guaranteed, due to the inevitable hardware/software failures and human errors in thecloud.Many data integrity auditing schemes have been proposed to allow either the data owner or the Third Party Auditor (TPA) to check whether the data stored in the cloud is intact or not. These schemes focus on different aspects of data integrity auditing, such as data dynamic operation [3–5], the privacy protection of data and user identities [6–8], key exposure resilience [9–11], the simplification of certificate management [12, 13] and privacy-preserving authenticators [14], etc. In the above data integrity auditing schemes, the user needs to generate authenticators for data blocks with his private key. It means that the user has to store and manage his private key in a secure manner [15]. In general, the user needs a portable secure hardware token (e.g. USB token, smart card) to store his private key and memorizes a password that is used to activate this private key. The user might need to remember multiple passwords for different secure applications in practical scenarios, which is not user friendly. In addition, the hardware token that contains the private key might be lost. Once the password is forgotten or the hardware token is lost, the user would no longer be able to generate the authenticator for any new data block. The data integrity auditing will not be functioning as usual. Therefore, it is very interesting and appealing to find a method to realize data integrity auditing without storing the privatekey.

2.EXISTINGSYSTEM

In Existing system, users can store their data in the cloud to avoid the expenditure of local data storage and maintenance. To ensure the integrity of the data stored in the cloud, many data integrity auditing schemes have been proposed. In most, if not all, of the existing schemes, a user needs to employ his private key to generate the data authenticators for realizing the data integrity auditing. Thus, the user has to possess a hardware token (e.g. USB token, smart card) to store his private key and memorize a password to activate this private key.

3.SYSTEM DESIGN

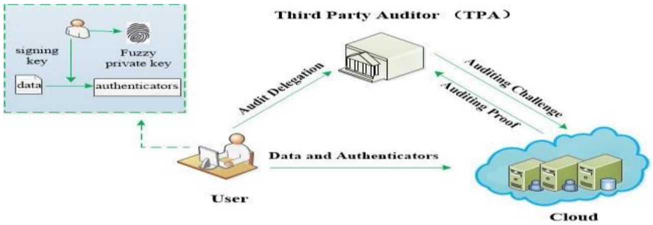

Fig. 1. System model of our data integrity auditing

BilinearMaps

Assume G1 and G2 are two multiplicative cyclic groups which have the same prime order p. A map e : G1 × G1 → G2 is called bilinear map if it satisfies the following properties: a) Bilinearity: for all u, v ∈ G1 and a, b ∈ Z ∗ p , e u a , vb = e(u, v) ab . b) Non-degeneracy: e (g, g) 6= 1, where g is a generator of G1. c) Computability: there exists an efficiently computable algorithm for computing map e : G1 × G1 → G2. Let PPGen be a bilinear groups generation algorithm (referred to as a bilinear group generator) which takes 1 k (k is a security parameter) as input, and generates a description of bilinear groups P P = (p, G1, G2, g,e).

SecurityAssumption

The security of our proposed scheme is based on the following security assumptions: Computational Diffie-Hellman (CDH) Problem. Given g, g x and h ∈ G1, where x ∈ Z ∗ p is unknown, compute h x ∈G1. Definition 1: (Computational Diffie-Hellman (CDH) Assumption) The advantage of a probabilistic polynomial time algorithm A in solving the CDH problem in G1 iAdvCDHA = P r[A(g, gx , h)= h x : x R ← Z ∗ p , h R ← G1]. The probability is taken over the choice of x and h, and the coin tosses of A. The CDH assumption means, for any polynomial time algorithm A, the advantage that A solves the CDH problem in G1 is negligible. Discrete Logarithm (DL) Problem. Given g, g x ∈ G1, where x ∈ Z ∗ p are unknown, compute x. Definition 2: (Discrete Logarithm (DL) Assumption) The advantage of a probabilistic polynomial time algorithm A in solving the DL problem in G1 is defined as AdvDLA = P r[A(g, gx) = x : x R ← Z ∗ p]. The probability is taken over the choice of x, and the coin tosses of A. The DL assumption means, for any polynomial time algorithm A, the advantage that A solves the DL problem in G1 is negligible.

Formalization of Fuzzy KeySetting

In a typical biometric authentication scheme [39], biometric data y = (y1, ..., yn) ∈ Y (Y is the metric space including all possible biometric data y) is extracted from a user in the phase of registration. In the phase of authentication, biometric data y 0= (y 0 1 , ..., y0 n) ∈ Y is extracted from a user. If y 0 is sufficiently close to y, we can conclude that the user who generated the biometric data y 0 and the user who generated the biometric data y are the same user; otherwise, they are different users. A fuzzy key setting FKS includes ((d, Y), γ, ε, Ω, θ) [37]. These symbols are defined asfollows:

a) (d, Y): This is a metric space, where Y (Y := [0, 1)n ⊂ Rn, R is the set of all real numbers) is the vector space including all possible biometric data y : (y1, ..., yn) ∈ Y, and d : Y × Y → Rn is the corresponding distance function. We define d(y, y 0) = maxi∈{1,...,n}|yi − y 0 i | for vectors y = (y1, ..., yn), y 0 = (y 0 1 , ..., y0 n) ∈Y.

b) γ: This is a uniform distribution of biometric data overY.

c) ε: This is the threshold value which belongs to R and is determined by a security parameter k (k = b−nlog2 (2ε)c). We set that p1 is the probability that two different users are accepted in the phase of identity authentication, it means that two different users are considered to be the same user. We require that this probability p1 is negligible in k based on ε. In other words, if the distance between two different biometric data y and y 0 is less than ε (that is d(y, y 0) < ε), the probability p1 is negligible ink.

d) Ω: This is an error distribution. If a user extracts biometric data y in the phase of registration,andextractsbiometricdatay0nexttime,y0 followsthedistribution{e←RΩ; y 0 ← y + e : y 0}. We can know that e is the “noise” of the biometric data extracted from the same user and the error distribution Ω is independent of individual. e) θ: This is an error parameter within [0, 1].

We can know that if y is the biometric data extracted from a user and e←RΩ is the “noise” of the biometric data extracted from the same user, y+e should be the biometric data extracted from the same user. We assume p2 is the probability that the same user is rejected in the phase of identity authentication, it means that a user is considered to be two different users. We require that the probability p2 is less than or equal to θ. That is, if d(y, y+e) ≥ ε, the probability p2.

Linearsketch

Let FKS = ((d, Y), γ, ε, Ω, θ) be a fuzzy key setting defined previously. We design a linear sketch scheme which is used to code and correct the error. This scheme is similar to the one-time pad encryption scheme. In a one-time pad encryption scheme, a plaintext m’s ciphertext c with a key sk is calculated as c = m + sk. The one-time pad encryption scheme satisfied the following property. For two ciphertexts c = m + sk and c 0 = m0 + sk with the same key sk, the “difference” 4m= m − m0 of plaintexts can be computed by comparing c and c 0 . In the designed linear sketch scheme, we make use of the above one-time pad encryption’s property. Thus, the process of coding in the linear sketch scheme can be viewed as the process of one-way encryption in the one-time pad encryption scheme, which is used to code the biometric data with a random value.

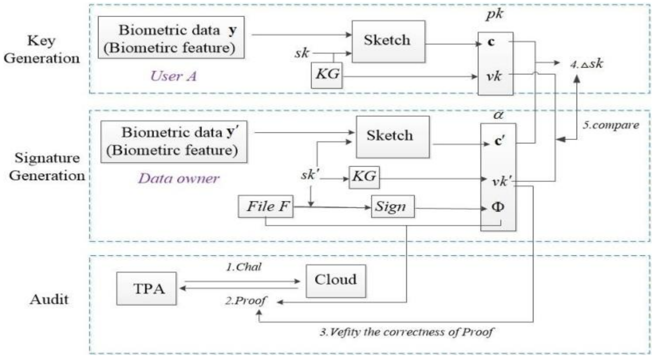

Fig. 2. An overview of data integrity auditing scheme without private key storage

4. Conclusion

In this paper, we explore how to employ fuzzy private key to realize data integrity auditing without storing private key. We propose the first practical data integrity auditing scheme without private key storage for secure cloud storage. In the proposed scheme, we utilize biometric data (e.g. fingerprint, iris scan) as user’s fuzzy private key to achieve data integrity auditing without private key storage. In addition, we design a signature scheme supporting blockless verifiability and the compatibility with the linear sketch. The formal security proof and the performance analysis show that our proposed scheme is provably secure and efficient.

5.REFERENCES

[1] H. Dewan and R. C. Hansdah, “A survey of cloudstorage facilities,” in *2011 IEEE World Congress on Services*, July 2011, pp.224–231.

[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” *IEEE Internet Computing*, vol. 16, no.1,pp.69–73,Jan2012.

[3] A. F. Barsoum and M. A. Hasan, “Provable multicopy dynamic data possession in cloud computing systems,” IEEE Transactions on Information Forensics and Secu- rity,vol.10,no.3,pp.485–497,March2015.

[4] 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.

[5] 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.

[6] 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.

[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 Secu- rity,vol.10,no.6,pp.1167–1179,2015.

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

[11] 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, Aug2017.

[12] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “Identity-based remote data possession checking in pub- lic clouds,” IET Information Security, vol. 8, no. 2, pp. 114–121, March2014.

[13] H. Wang, D. He, and S. Tang, “Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June2016.

[14] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong,and R. Hao, “Remote data possession checking with privacy-preserving 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.