Remote data integrity checking using Huffman hash tree (MHT) Scheme

Sk. Anjaneyulu Babu[1], Ravulakollu Venkatesh[2]

#1Associate Professor, Department of MCA at QISCET(Autonomous), Vengamukkapalem, Prakasam (DT)

#2PG Scholar in the Department of MCA at QISCET (autonomous), Vengamukkapalem, Prakasam (DT)

ABSTRACT_

The distant information ownership checking system can really confirm the honesty of reevaluated information, which can normally be partitioned into public confirmation and confidential confirmation. The verifier of public confirmation can be any cloud client, while private check must be the information proprietor. Nonetheless, in most commonsense circumstances, the information proprietor expects that main a particular verifier can perform honesty checking undertakings and that verifier can't acquire any information about the information. Yan et al. proposed a scheme for remote data possession verification that includes the designated verifier. This scheme can guarantee that only the designated verifier can verify the integrity of data, while other verifiers are unable to do so. However, issues of data privacy protection are not taken into account in this scheme, which is based on public key infrastructure technology. An identity-based remote data possession checking scheme that meets the requirement of the data owner to specify a unique verifier is what we propose as a means of overcoming these flaws. Besides, in this plan, we utilize an irregular whole number to dazzle information uprightness verification to safeguard information security and use Merkle hash tree construction to accomplish dynamic update of information. Simultaneously, our plan can stay away from the complicated endorsement the board openly key framework. We demonstrated the security of our plan in view of the discrete logarithm supposition and the computational Diffie-Hellman suspicion. Hypothetical examination and exploratory outcomes show that our plan is plausible and viable in useful applications.

1.INTRODUCTION

As a basic piece of distributed computing, distributed storage has drawn in an ever

increasing number of clients to re-appropriate their information to the cloud specialist co-op (CSP) because of its benefits of scale, adaptability, versatility, and financial advantages [1]. Be that as it may, cloud security issues can't be overlooked [2]. Users of the cloud are unable to monitor the status of their data because cloud storage reduces their physical control over the data. Due to various security threats, the CSP may knowingly conceal outsourced data loss or leakage. All the more truly, the CSP may purposefully erase information that clients don't utilize much of the time to save space to give capacity administrations to additional clients [3]. To confirm whether the information is put away totally in the cloud, numerous distant information ownership checking (RDPC) plans have been proposed.

As of now, a greater part of the current RDPC plans depend on open key framework (PKI) innovation. PKI innovation requires various declaration the executives activities like endorsement age, conveyance, capacity, check, and disavowal, expanding computational and correspondence costs. Furthermore, assuming pernicious programmers control the testament authority (CA), the security of PKI can barely be completely ensured. Identity-based cryptography (IBC) was developed to address this issue. In IBC innovation, the client's public key is its personality (ID number, email address, and other data that remarkably distinguishes the client), staying away from the presentation and the board of public-key endorsements. As a result, constructing an RDPC scheme with IBC is more secure and efficient.

RDPC schemes can be divided into the following groups based on the identity of the verifier: public verification [6] and private verification [7] In private verification, only the owner of the data can be the verifier; in public verification, any cloud user can verify the integrity of the data. Assuming that private confirmation is utilized, the information proprietor requirements to perform unwieldy checking routinely, which builds the computational expense. What's more, the decency and authority of the checking results may likewise be impacted. Consequently, most RDPC plans utilize public confirmation to actually take a look at reevaluated information. However, the verifier also introduces new security requirements. The verifier might be interested about reevaluated information and will attempt to get a few information content during the trustworthiness checking. The owner of the data cannot tolerate the verifier's curiosity if the data

stored in the cloud is private or confidential. Along these lines, information security assurance is fundamental. Encoding _les before information rethinking can lighten information security issues, yet this approach expands the handling trouble for the information proprietor. Key management problems arise as a result, and data breaches can still occur when decryption keys are exposed. Additionally, for shared information, the scrambled information can't be utilized by different clients. Accordingly, it is important to consider the information security insurance issues.

In numerous reasonable circumstances, the information proprietor might hope to assign a particular verifier to really look at reevaluated information, while different verifiers can't perform such work. A user, for instance, has previously independently verified private data that was outsourced. Be that as it may, he is limited from riding the Web and can't perform private confirmation since he is on the combat zone. In this instance, he intends to appoint a reliable verifier to examine the outsourced data. Also, on the grounds that the information is private, the client doesn't believe the verifier should get the information content. Another model is an organization putting away its business data in the cloud. Its rivals might counterfeit personalities to check information and acquire business data about the organization. Thusly, the organization needs to assign a verifier, and because of the secrecy of business data, it requirements to think about information security insurance. In both of the above cases, private or public confirmation doesn't make a difference. Yan and others 8] proposed a plan to guarantee that main the assigned verifier can really take a look at the information honesty.

Since rethought information isn't generally static, and the information proprietor might have to refresh information often, supporting unique information operations is basic. We work on the plan in [8] and propose a personality based RDPC conspire with the assigned verifier that upholds security assurance and dynamic information tasks, which can more readily adjust to the genuine circumstance

2.LITERATURE SURVEY

2.1 Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage

Abstract

Remote data integrity checking (RDIC) enables a data storage server, say a cloud

server, to prove to a verifier that it is actually storing a data owner's data honestly. To date, a number of RDIC protocols have been proposed in the literature. However, most of the constructions suffer from the issue of requiring complex key management. That is, they rely on the expensive public key infrastructure (PKI), which might hinder the deployment of RDIC in practice. In this paper, we propose a new construction of identity-based (ID-based) RDIC protocol by making use of key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based RDIC schemes. We formalize ID-based RDIC and its security model including security against a malicious cloud server and zero knowledge privacy against a third party verifier. The proposed ID-based RDIC protocol leaks no information of the stored data to the verifier during the RDIC process. The new construction is proven secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier. Extensive security analysis and implementation results demonstrate that the proposed protocol is provably secure and practical in the real-world applications

2.2 Privacy-preserving public auditing for data integrity in cloud

M Shaik Saleem and M Murali

Abstract.

Cloud computing which has collected extent concentration from communities of research and with industry research development, a large pool of computing resources using virtualized sharing method like storage, processing power, applications and services. The users of cloud are vend with on demand resources as they want in the cloud computing. Outsourced file of the cloud user can easily tampered as it is stored at the third party service providers databases, so there is no integrity of cloud users data as it has no control on their data, therefore providing security assurance to the users data has become one of the primary concern for the cloud service providers. Cloud servers are not responsible for any data loss as it doesn’t provide the security assurance to the cloud user data. Remote data integrity checking (RDIC) licenses an information to data storage server, to determine that it is really storing an owners data truthfully. RDIC is composed of security model and ID-based RDIC where it is responsible for the security of every server and make sure the data privacy of cloud user against the third

party verifier. Generally, by running a two-party Remote data integrity checking (RDIC) protocol the clients would themselves be able to check the information trustworthiness of their cloud. Within the two party scenario the verifying result is given either from the information holder or the cloud server may be considered as one-sided. Public verifiability feature of RDIC gives the privilege to all its users to verify whether the original data is modified or not. To ensure the transparency of the publicly verifiable RDIC protocols, Let's figure out there exists a TPA who is having knowledge and efficiency to verify the work to provide the condition clearly by publicly verifiable RDIC protocols.

3.PROPOSED SYSTEM

The RDPC technique with the designated verifier in [8] is improved by the approach that is proposed in this study. We suggest a novel RDPC scheme in light of the PKI's intricate certificate management procedures and the verifier's semi-trusted difficulty. The following are this paper's main contributions:

1) We construct an RDPC scheme with a designated verifier based on IBC technology, avoiding the certificate administration issue.

2) Data privacy is achieved by our plan. The CSP blinds the data integrity proof using a random number, preventing the verifier from obtaining any data content.

3) To support dynamic data operations and adhere to the needs of rapid data changes, our approach makes use of the Merkle hash tree (MHT).

4) We demonstrate the security of our approach and assess its communication and computation costs. Finally, test results demonstrate that our plan is feasible and more effective.

3.1 IMPLEMENTATION

3.1.1 Data Owner

In this module, the patient shares the PHRs with the department byencrypt the PHRs data under the department's identityid, then upload the ciphertext to the medical server and performs the following operations such as Register and Login, Upload File, Check Data Integrity, View Verifier Results, View Uploaded Files Details.

3.1.2 User

In this module, he logs in by using his/her user name and password. After interacting with the doctors, the superintendent decrypts the ciphertext and outputs the

PHRs. After Login receiver will perform operations like Register and Login, Search File.

3.1.3 KGC

In this module, the sector can do following operations Login, View All Files and Generate Secret Key.

3.1.4 Verifier

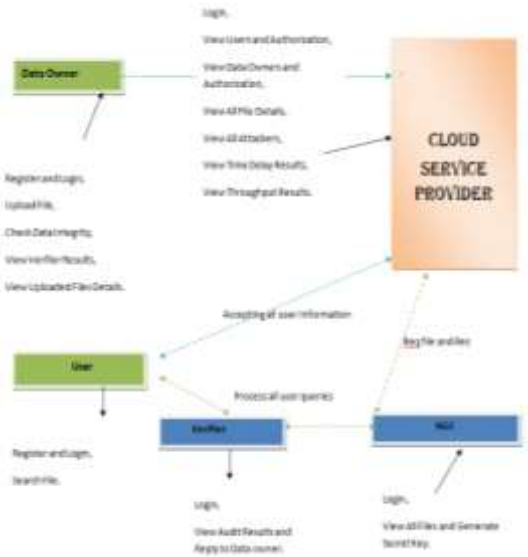

Fig 1: Architecture

4.RESULTS AND DISCUSSION

Schemes	The designated verifier	Privacy protection	Dynamic data operations	Type
Scheme in [8]	Yes	No	No	PKI
Scheme in [11]	Yes	No	No	PKI
Scheme in [12]	Yes	No	No	PKI
Scheme in [13]	Yes	No	No	PKI
Scheme in [22]	No	Yes	No	IBC
Scheme in [23]	No	Yes	No	IBC
Scheme in [25]	No	No	Yes	IBC
Scheme in [27]	No	Yes	Yes	PKI
Scheme in [29]	No	Yes	Yes	PKI
Scheme in [30]	No	Yes	Yes	PKI
Our scheme	Yes	Yes	Yes	IBC

In this module, the Superintendent can do following operations like Login, View Audit Results and Reply to Data owner.

3.1.4 Cloud Service Provider

The cloud Server manages a server to provide data storage service and can also do the following operations such as Login, View Users and Authorization, View Data Owners and Authorization, View All File Details, View All Attackers, View Time Delay Results, View Throughput Results.

TABLE 1: Functionality comparison with related schemes

We carry out a useful correlation of our plan with a few related plans, as displayed in Table 1. In terms of the designated verifier, the schemes in [8], [11], and [13] either use an authorization or embed the verifier information into the tags. Notwithstanding, different plans in Table 1 utilize public confirmation that any verifier can per structure really taking a look at undertakings. As far as security insurance, plans in [22], [23], [27] and [30] consolidates homomorphic veri fication with arbitrary veil, and plan in [29] encodes and afterward signs the information block, all of which guarantee that the verifier doesn't realize anything about the information content during the information trustworthiness checking. In any case, different plans in Table 1 don't

consider that processing the straight mix of information blocks in the information trustworthiness confirmation might derive the information content. As far as unique information activities, plans in [25], [29] and [30] separately embrace various information designs to help information refreshes actually. When dynamic data streams arrive, the authentication data structure defined by the schemes in [27] can be adaptively extended. By the by, different plans center around static information and furthermore can't be straightforwardly stretched out to dynamic information plans. The identity of the user serves as the basis for the IBC schemes described in [22], [23], and [25]. How ever, different plans depend on PKI innovation, which requires an endorsement gave by the CA to guarantee the validness of the client's public key. Furthermore, our plan is the only one that can fulfill all of the aforementioned functions.

5.CONCLUSION

This study suggests a verifier-designated identity-based remote data integrity checking scheme. This plan can also achieve data privacy protection and resolve the semi-trusted verifier problem. For dynamic operations like data insertion, modification, and deletion, our approach makes advantage of MHT. We further demonstrate the security of the system using the DL assumption and the CDH assumption. Finally, the experimental analysis demonstrates that our system is efficient and better suited to scenarios for real-world application.

REFERENCES

[1] M. Armbrust, A. Fox, R. Grif_th, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, ``A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50_58, Apr. 2010.

[2] D. Zissis and D. Lekkas, ``Addressing cloud computing security issues," Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583_592, Mar. 2012.

[3] J. Lu, F. Nan, Y. Huang, C.-C. Chang, Y. Du, and H. Tian, ``Privacy- preserving public auditing for secure data storage in fog-to-cloud computing," J. Netw. Comput. Appl., vol. 127, pp. 59_69, Dec. 2018.

[4] Y. Deswarte, J.-J. Quisquater, and A. Saidane, ``Remote integrity checking," in Proc. Work. Conf. Integrity Internal Control Inf. Syst., Cham, Switzerland: Springer, 2003, pp. 1_11.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D.

Song, ``Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598_609.

[6] B. Wang, B. Li, and H. Li, ``Panda: Public auditing for shared data with efcient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92_106, Jan./Feb. 2015.

[7] Y. Feng, Y. Mu, G. Yang, and J. K. Liu, ``A new public remote integrity checking scheme with user privacy," in Proc. Australas. Conf. Inf. Secur. Privacy. Berlin, Germany, Springer, 2015, pp. 377_394.

[8] H. Yan, J. Li, and Y. Zhang, ``Remote data checking with a designated veri_er in cloud storage," IEEE Syst. J., vol. 14, no. 2, pp. 1788_1797, Jun. 2020.

[9] A. Juels and B. S. Kaliski, ``Pors: Proofs of retrievability for largeles," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584_597.

[10] H. Shacham and B. Waters, ``Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Berlin, Germany, Springer, 2008, pp. 90_107.

[11] Y. Ren, J. Xu, J. Wang, and J.-U. Kim, ``Designated verifer provable data possession in public cloud storage," Int. J. Secur. Appl., vol. 7, no. 6, pp. 11_20, Nov. 2013.

[12] S.-T. Shen and W.-G. Tzeng, ``Delegable provable data possession for remote data in the clouds," in Proc. Int. Conf. Inf. Commun. Secure., Berlin, Germany, Springer, 2011, pp. 93_111.

[13] H.Wang, ``Proxy provable data possession in public clouds," IEEE Trans. Services Comput., vol. 6, no. 4, pp. 551_559, Oct./Dec. 2013.

[14] H. Wang, ``Identity-based distributed provable data possession in multi- cloud storage," IEEE Trans. Services Comput., vol. 8, no. 2, pp. 328_340, Mar./Apr. 2015.

[15] J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, ``RKA security for identity-based signature scheme," IEEE Access, vol. 8, pp. 17833_17841, 2020.

[16] Y. Chen and J. Chang, ``Identity-based proof of retrievability meets with identity-based network coding," Cluster Comput., early access, 2022, doi: 10.1007/s10586-022-03545-y.

[17] J. Zhao, C. Xu, F. Li, and W. Zhang, ``Identity-based public verification with privacy-preserving for data storage security in cloud computing," IEICE Trans. Fundam. Electron. Commun.

Comput. Sci., vol. 96, no. 12, pp. 2709_2716, 2013.

[18] Y. Ji, B. Shao, J. Chang, and G. Bian, ``Privacy-preserving certicateless provable data possession scheme for big data storage on cloud, revisited," Appl. Math. Comput., vol. 386, Dec. 2020, Art. no. 125478.

[19] X. Yang, M. Wang, T. Li, R. Liu, and C. Wang, ``Privacy-preserving cloud auditing for multiple users scheme with authorization and traceability," IEEE Access, vol. 8, pp. 130866_130877, 2020.

[20] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacy- preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013.

AUTHOR PROFILE

SK. ANJANEYULU BABU, Associate Professor in the department of MCA at QIS College Engineering and Technology. He is having over 20 Research publications. His area of interest is Cloud Computing, Machine learning &Data mining.

RAVULAKOLLU VENKATESH, PG Scholar in the department of MCA, QIS College of engineering and Technology (Autonomous), Vengamukkapalem, Prakasam (DT). His areas of Interests are Networking & Cloud Computing.