International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-8, Issue-4, July 2020
https://doi.org/10.21276/ijircst.2020.8.4.9
www.ijircst.org

Efficient Data Integrity and Auditing in Cloud by using Block Chain

Prof. Chethan Raj C, Shivani M S, Sowjanya D R, Sowmya M T, Tejaswini R

ABSTRACT- The main aim of this paper is to discuss the usage of cloud storage services, enabling individuals to store their information in the cloud and keep away from the local data storage and maintenance expense. Numerous data integrity auditing systems have been implemented to guarantee the quality of the data stored in the cloud. An individual would like to enroll his private key to create the authenticators for understanding the auditing of data integrity in certain, but not all of the current system. The user must then have a hardware token (e.g. USB token, smart card) for storing the private key and memorizing a password to trigger the private key. Most of the new data integrity auditing system will be unable to operate if the user misplaced this hardware token or forgot this password. We are proposing a new module called data integrity auditing without private key storage to solve this issue, and developing such a scheme using block chain technology. In this project we are proposing a computerized signature along with face reorganization with block chain operation, so that there will be no unique design to obtain unauthorized and furthermore to prevent hacking operation and all the respective user data or information will be stored in cloud with maximum security.

Manuscript received July 20, 2020

Prof Chethan Raj C, Associate Professor, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India (email:chethanraj016@gmail.com)

Shivani M S, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India

Sowjanya D R, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India

Sowmya M T, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India

Tejaswini D R, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India

KEYWORDS- Cloud storage, Data integrity auditing and Data security Biometric data.

I. INTRODUCTION

Using cloud storage services, users can store their data within the cloud to avoid the expenditure of local data storage and maintenance. However, once the user uploads their data to the cloud, they will lose the physical control of their data since they no longer keep their data in local [1]. To ensure the integrity of the info stored within the cloud, many data integrity auditing schemes are proposed. Shen et al. [6] designed a light-weight data integrity auditing scheme, which introduced a Third Party Medium to generate authenticators and verify data integrity on behalf of users. It mainly focus on different aspects of data integrity auditing such as data dynamic operation [5], key exposure resilience [3&8], the simplification of certificate management [10] and also proposes a privacy-aware remote data integrity auditing scheme for shared data [4]. In most, if not all, of the prevailing schemes, a user must employ his private key to get the info authenticators for realizing the info integrity auditing. Thus, the user has to possess a hardware token (e.g. USB token, smartcard) to store his private key and memorize a password to activate this private key. If this hardware token is lost or this password is forgotten, most of the present data integrity auditing schemes would be unable to figure [14]. In order to overcome this problem, we propose an paradigm called data integrity auditing without private key storage and design such a scheme. In this scheme, we use biometric data (e.g. iris scan, fingerprint) because the user's fuzzy private key to avoid using the hardware token. Unfortunately, biometric data is measured with inevitable noise each time and cannot be reproduced precisely since some factors can affect the change of biometric data. For example, the finger of each person will generate a different fingerprint image every time due to pressure, moisture, presentation angle, dirt, different sensors, and soon. Therefore, the biometric data cannot be used directly as the private key to generate authenticators in data integrity auditing. Meanwhile, the scheme can still effectively complete the info integrity auditing. We utilize a linear sketch with coding and error correction processes to verify the identity of the user. Additionally, the paper designs a

new signature scheme which not only supports block less verifiability, but also is compatible with the linear sketch. The security proof and therefore the performance analysis show that our proposed scheme achieves desirable security and efficiency. The Block chain is the technology that underpins crypto currencies such as Bit coin. Fundamentally, the block chain is just a ledger, a digital record of transactions related to a digital currency, a Bit coin, as an example. It is an open system that does not require a trusted third party as all transactions are logged in an immutable distributed public ledger that requires no central repository of data, it is entirely decentralized. Block chain-based applications are arising, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of block chain technology like scalability and security problems waiting to be overcome. And this paper presents a comprehensive overview on block chain technology. We provide a summary of block chain architecture firstly and compare some typical consensus algorithms utilized in different block chains.

II. RELATED WORK

A. Data Integrity Auditing without Private Key Storage for Secure Cloud Storage, Wenting Shen, Jing Qin [1]

In this paper, they explore how to employ 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. The formal security proof and the performance analysis shows their proposed scheme is provably secure and efficient.

B. Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data,Yue Zhang[2]

In the paper the author has discussed numerous topic about cloud storage and auditing techniques. Cloud storage auditing schemes for shared data ask checking the integrity of cloud data shared by a gaggle of users. User revocation is usually supported in such schemes, as users could also be subject to group membership changes for various reasons. Previously, the computational overhead for user revocation in such schemes is linear with the entire number of file blocks possessed by a revoked user.

C. Storage Key-Exposure Resilient Auditing for Secure Cloud Storage, Jia Yu[3]

Key exposure is one of the serious security problems for cloud storage auditing. In order to affect this problem, cloud storage auditing scheme with key-exposure resilience has been proposed. They propose a new paradigm called strong key-exposure resilient auditing scheme for secure cloud storage. In this paradigm, the security of the cloud storage auditing not only earlier than but also later than the key exposure can be preserved.

D. NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users, Anmin Fu [4]

In this paper, they propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a holomorphic verifiable group signature. Moreover, the scheme ensures that group users can trace the data changes through the designated binary tree and may recover the newest correct data block when the present data block is broken. During the process of auditing, the third party auditors cannot obtain the identities of the signers, which ensures the identity privacy of the group users. Therefore, it eliminates the abuse of single authority power and ensures non-frame ability. Exceptionally, group users can trace the data changes through the designed binary tree and recover the latest correct data block when the current data block is damaged.

E. RITS-MHT: Relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing, Seema Bhava [5]

In this, paper they propose an approach based on Relative Index and Time Stamped MerkleHash Tree which integrates with relative index of a node resulting in reduction of computation cost of searching a knowledge block from O(n) in Wang's protocol to O(log n) and time of last modification to data, thereby guarantying freshness of knowledge respectively. This protocol supports public auditing of knowledge, and efficiently supports data dynamic operations like insertion, modification, deletion of outsourced data at minimal computational cost. The relative index of a node has been integrated with the hash value of the node in tree to reduce searching complexity. This guarantees that whenever a data file is accessed by a user it is the most recent copy of data.

F. Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium, Rong Hao[6]

In this scheme, they introduce a Third Party Medium to perform time-consuming operations on behalf of users. In this paper, they propose a light-weight and privacy-preserving secure cloud auditing scheme for group users, which can greatly reduce the computation burden on the user side. The scheme can protect the data privacy against the Third Party Medium by blinding data in the phase of data uploading and data auditing.

G. Data Possession Checking with Privacy-Preserving Authenticators for Cloud Storage, Fanyu Konhg [7]

In this paper, they propose a new paradigm named remote data possession checking with privacy-preserving authenticators for cloud storage. In this new paradigm, both cloud service provider and the public verifier do not have access to the real authenticators for cloud data. To securely protect the privacy of the authenticator, they design a new authenticator called Homomorphic Invisible Authenticator, which protects the privacy of authenticator and supports the block less verification. Based on Homomorphic Invisible

Authenticator, they construct the first remote data possession checking scheme with privacy-preserving authenticators for cloud storage. The results show that the proposed paradigm is secure and efficient.

H. Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates, Cong Wang[8]

In this paper, they specialize in the way to make the key updates as transparent as possible for the client and propose a replacement paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this paradigm, key updates are often safely outsourced to some authorized party, and thus the key-update burden on the client are going to be kept minimal. Specifically, they leverage the third party auditor in many existing public auditing designs. In this case third party auditor play the role of authorized party and make it responsible of both the storage auditing and therefore the secure key updates for key-exposure resistance. In this design, third party auditor only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the third party auditor when uploading new files to cloud.

I. Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud, Zheming Dong[9]

In this paper, we have proposed two privacy-preserving public auditing protocols for secure storage in cloud environment. Our protocols are based on online/offline signatures, by which a user only needs to perform lightweight computing when a data file to be outsourced is given. Further, our protocols also support batch auditing and data dynamics. Simulation shows that our protocol is much more efficient than a recent privacy preserving public auditing protocol. Thus, we believe that our protocols are practical for those end devices with low computation capabilities.

J. Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud, Shaohua Tang[10]

In this paper, they propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: IDPUIC (identity-based proxy-oriented data uploading and remote data integrity checking in public cloud). They give the formal definition, system model and security model. Then, a concrete IDPUIC protocol is designed by using the bilinear pairings. The proposed ID-PUIC protocol is provably secure supported the hardness of computational Diffie-Hellman problem. The IDPUIC protocol is also efficient and flexible. Based on the first client's authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking.

III. EXISTING SYSTEM

- The existing system employs the random sample technique and homomorphic linear authenticators to design a PDPscheme, which allows an auditor to verify the integrity of cloud data without downloading the whole data from the cloud. The Proof of Retrievability (PoR)Ateniese et al. [13].In the proposed scheme, the error correcting codes and the spot-checking technique are utilized to ensure the retrievability and the integrity of the data stored in the cloud.
- The existing system implements private verifiability and public verifiability by using pseudorandom function and BLS signature, Liu et al [12].To support user-interactions, including data modification, insertion and deletion, constructed a dynamic data integrity auditing scheme by exploiting the index hash tables.
- In public data integrity auditing, The TPA might derive the contents of user's data by challenging the same data blocks repeated times.
- To protect the data privacy exploited the random masking technique to construct the first public data integrity auditing scheme supporting privacy preserving. Li et al. [9].
- To relieve the user's computation burden of authenticator generation, a data integrity auditing scheme using in distinguishability obfuscation technique, which reduces the overhead for generating data authenticators Guan et al [11].

IV. DRAWBACK OF EXISTING SYSTEM

- In the existing system, there are no accurate data integrity proof results. The system's security is extremely less thanks to lack of BLS Short Signature for data blocks.
- The user's computation burden of authenticator generation.
- The data integrity auditing scheme which preserves data privacy from the TPA proposed a cloud storage auditing scheme Zhang et al. [2] with perfect data privacy preserving by making use of zero- knowledge proof.
- The problem of data dynamics in data integrity auditing and designed a data integrity auditing scheme supporting data dynamic operations based on the Divide and Conquer Table.

V. OVERVIEW OF THE PROPOSED SCHEME

- The system mainly aim to design a practical data integrity auditing scheme without private key storage for secure cloud storage.
- In our scheme, two fuzzy private keys (biometric data) are extracted from the user in the phase of registration and the phase of signature generation. We respectively use these two fuzzy private keys to generate two linear sketches that contain coding and error correction processes.

- In order to confirm the user's identity, we compare these two fuzzy private keys by removing the "noise" from two sketches. If the two biometric data are sufficiently close, we can confirm that they are extracted from the same user; otherwise, from different users. The design a signature satisfying both the compatibility with the linear sketch and the block less verifiability is a key challenge for realizing data integrity auditing without private key storage.
- In order to overcome this challenge, we design a new signature scheme called as MBLSS by modifying the BLS short signature based on the idea of fuzzy signature. We give the safety analysis and justify the performance via concrete implementations. The results show that the proposed scheme is secure and efficient.

VI. ADVANTAGES OF PROPOSED SYSTEM

- An affective technique to ensure that when the cloud properly stores users' data, the proof it generates can pass the verification of the TPA.
- An efficient technique to assure that if the cloud doesnot possess user intact data, it cannot pass the verification of the TPA.
- Secure and efficient techniques to allow the user to utilize biometric data as fuzzy private key to accomplish data integrity auditing without private key storage.

VII. ARCHITECTURE DIAGRAM

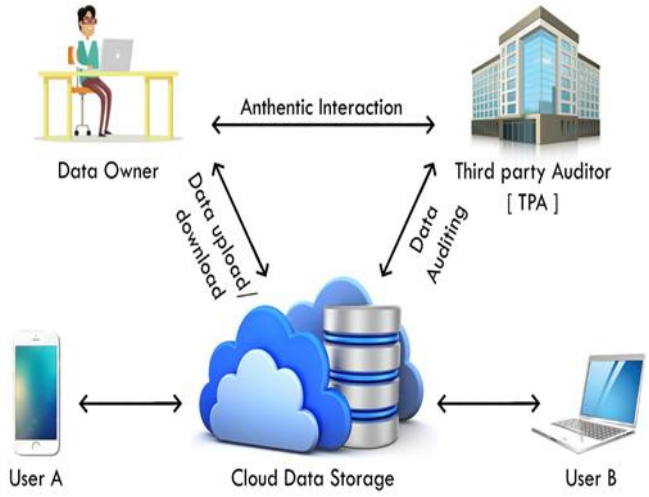

Fig 1: System diagram

Today, most of the individuals and organizations use cloud storage to remote store their data and luxuriate in the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and their maintenance.
The data auditing method for distributed cloud servers consist of four entities. As follow:

(1) Data Owner (DO): the one that uploads his/her data to the cloud space.
(2) Cloud Service Provider: who has amount of computing resources and stores and manages DOs data. The CSP is additionally liable for managing cloud servers.
(3) Third Party Auditor (TPA): In order to alleviate the computation burden on data owner's side, the auditing process is often assigned to a TPA with adequate skills and capabilities to accomplish the auditing task on behalf of the data owner. The TPA's role is especially important when data owners possess relatively poor computer in terms of processing power, space for storing and bandwidth. While TPA is considered a trustful and reliable entity it'd be inquisitive at an equivalent time. Consequently, one significant countermeasure during data auditing is to prevent TPA obtaining knowledge of data owner's data content and protect privacy of data.
(4) User (individual or enterprise): Who is enrolled and authenticated by the DO and permitted to have pre-determined type of access on the outsourced data (refer to Sookhak et al.). The architecture of DA when TPA is involved is shown in Figure 1.

VIII. METHODOLOGY

A. DATA OWNER

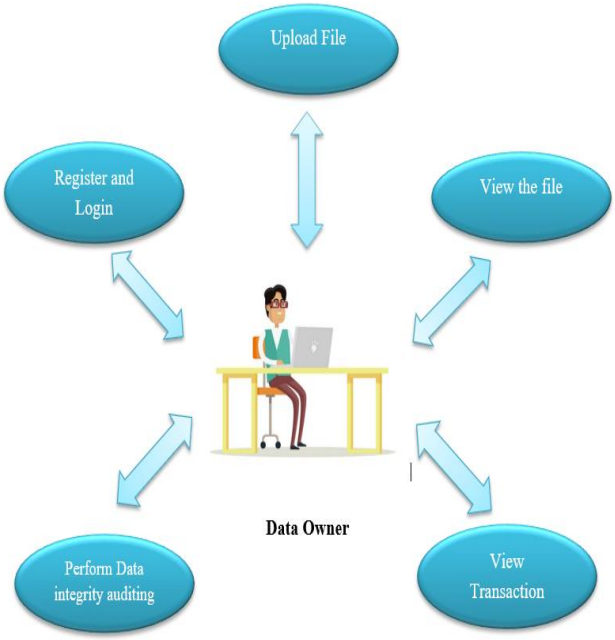

Fig 2: Data Owner

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Upload File with Blocks, View All Upload File with Blocks, Perform Data Integrity Auditing and View Transactions.

B. CLOUD SERVER

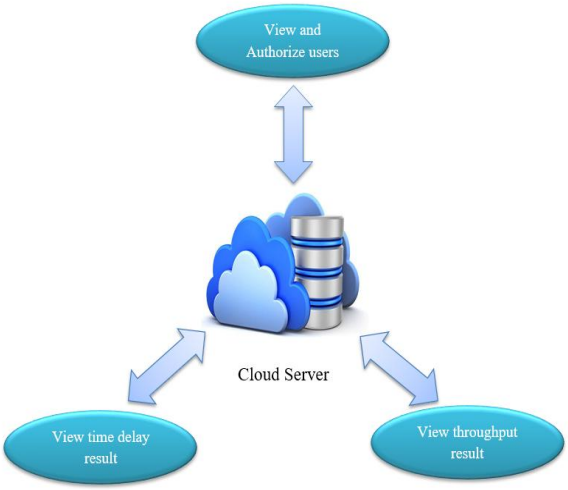

Fig 3: Cloud Access

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View and Authorize Users, View and Authorize Owners, View All File's Blocks, View All Transactions, View All Attackers, View Time Delay Results, View Throughput Results.

C. TPA

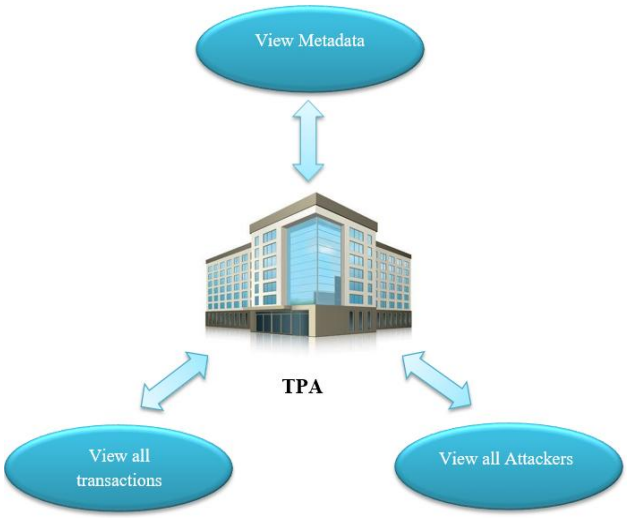

Fig 5: Trusted Party Authority

In this module, the TPA performs the following operations such as View Metadata Details, View All Transactions and View All Attackers.

D. END USER

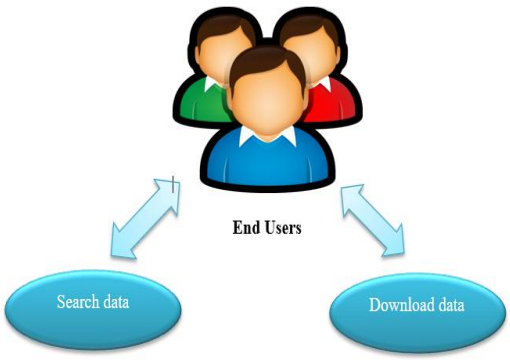

Fig 4: End user Interface

In this module, the user has to register to cloud and log in and performs the following operations such as Search Data, Download Data.

IX. ALGORITHM

A data integrity auditing scheme without private key storage consists of the following five algorithms: Setup, KeyGen, SignGen, ProofGen and ProofVerify. Specifically, these algorithms are described as follows:

- Setup(1^k , FKS): This algorithm takes fuzzy key setting FKS and a security parameter kas input. It outputs the public parameter pp^1.
- KeyGen(pp^1, y): This algorithm takes public parameter pp^1 and the biometric data y $\in R^n$as input. It generates p^k as his public key, which including a sketch c and a verification key vk.
- SignGen(y^1, F): This algorithm takes the biometric data $y^1 \in R^n$ and the file Fas input. It outputs a signature α which includes the verification key vk^1, the sketch c^1 and the set of authenticators Φ.
- ProofGen(F, Φ, chal): This algorithm takes the file F, the corresponding authenticator set Φ and the auditing challenge chalas input. It outputs an auditing proof P that proves the cloud indeed keeps this file.
- ProofVerify(pk, chal, P, vk^1 , c^1): This algorithm takes the user's public key pkas input, the auditing challenge.

X. RESULT ANALYSIS

In the paper the data integrity is checked using Block chain in cloud and also allowing the secure payment to be finished without any bank or any intermediary and services such as digital assets, remittance and online payment. The block chain has to solve the Storage optimization of block chain & Redesigning block chain.

XI. SCOPE

In Digital signature each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the entire network. The typical digital signature is involved with two phases: signing phase and verification phase, hence block chain plays important role of decentralized transaction and data management technology and it has following key characteristics Decentralization, Persistency, Anonymity and Auditability.

XII. MOTIVATION

- When the client transfer their information to the cloud, they cannot get to information physically since, their information will not in neighborhood.
- In information astuteness inspecting conspire, the client should produce authenticators for information squares with his private key. It means that the client must store and oversee his private key in a secure way on the off chance that client in capable to memorize their password and any misfortune in hardware tokens, the client would not be able to create the authenticator for any modern information square.
- There may be a challenge is to plan a signature fulfilling both the compatibility with the straight portray and the block less unquestionable status.

XII. CONCLUSION

In this paper, we investigate how to utilize fuzzy private key to realize data integrity auditing without putting away 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 information (e.g. fingerprint, iris check) as user's fuzzy private key to attain data integrity auditing without private key capacity. In expansion, we design a signature conspire supporting block less verifiability and the compatibility with the direct outline. The formal security proof and the execution examination appear that our proposed scheme is provably secure and productive. Block chain shows their potential for transforming traditional industry with its key feature: decentralization, persistency, anonymity and auditability. In future the block chain associated concept &some possible future directions are also proposed. Nowadays block chain based applications are arising and that we decide to conduct in-depth investigations on block chain-based applications within the future. The goal of Block chain is to supply anonymity, security, privacy, and transparency to all or any its users. However, these attributes set up a lot of technical challenges and limitations that need to be addressed.

ACKNOWLEDGMENT

I thank our mentor **Prof.Chethan Raj C** for analyzing the data and advised on all aspects related to cloud storage, data integrity auditing, the other concept and validated the experimental results and reviewed the paper.

REFERENCES

[1] Wenting Shen, Jing Qin"Data Integrity Auditing without Private Key Storage for Secure Cloud Storage" A review IEEE Trans.2019.

[2] Yue Zhang "Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data" A review IEEE Trans. 2018.

[3] Jia Yu "Storage Key-Exposure Resilient Auditing for Secure Cloud Storage" A review IEEE Trans. 2017.

[4] Anmin Fu, Huaqun Wang, Shui Yu, Chanyinghusang "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users: A review"IEEE Trans. 2017.

[5] Neeru Garg, Seema Bhava" RITS-MHT: Relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing: A review" 2017.

[6] Wenting Shen, Jiayu, Hui Xia, Rong Hao" Light-Weight and Privacy-Preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium: A review" 15 Jan 2017.

[7] Wenting Shen, Hanlin Zhang, Rong Hao, Fanyu Konhg "Data Possession Checking with Privacy-Preserving Authenticators for Cloud Storage: A review" 2017.

[8] Jia Yu, Kui Ren, Cong Wang" Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates: A review "IEEE Trans. 2016.

[9] Jiangtao Li, Lei Zhang, Joseph K. Liu, Zheming Dong" Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud: A review" IEEE Trans. 2016.

[10] Huaqun Wang, Debiao He, Shaohua Tang" Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud: A review" 2016.

[11] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Cham: Springer International Publishing, 2015.

[12] C. Liu, J. Chen, L. Yang, et al, "Authorized public auditing of dynamicbig data storage on cloud with efficient verifiable fine-grained updates,"IEEE Transactions on Parallel and Distributed Systems 2014.

[13] 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 2007.

[14] C. Ellison and B. Schneier, "Ten risks of pki: What you're not being told about public key infrastructure,"2000.

ABOUT THE AUTHORS

Prof. Chethan Raj C, Associate Professor,Research Scholar, Dept. of CSE, Mysuru Royal Institute of technology, Mandya

Shivani M S, Dept. of CSE Mysuru Royal Institute of technology, Mandya

Sowjanya D R, Department of CSE, MysuruRoyal Institute of technology, Mandya

Sowmya M T, Department of CSE, Mysuru Royal Institute of technology, Mandya

Tejaswini R, Department of CSE, Mysuru Royal Institute of technology, Mandya

