IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

PROVABLY SECURE AND LIGHTWEIGHT IDENTITYBASED AUTHENTICATED DATA SHARING PROTOCOL FOR CYBER CLOUD ENVIRONMENT

Aniket Vishwakarma, Avinash A Undri, Dhanush M, Sanjay Mandal

Student Student Student Student
Computer Science and Engineering,
East Point College of Engineering and Technology, Bengaluru, India

Abstract: Secure and efficient file storage and sharing via authenticated physical devices remain challenging to achieve in a cyber- physical cloud environment, particularly due to the diversity of devices used to access the services and data. Thus, in this project, we present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients. The proposed protocol is demonstrated to resist chosen-ciphertext attack (CCA) under the hardness assumption of decisional- Strong Diffie Hellman (SDH) problem. We also evaluate the performance of the proposed protocol with existing data sharing. Protocol in terms of computational overhead, communication overhead and response time

1. INTRODUCTION

Cloud storage auditing is used to verify the integrity of the data stored in public cloud, which is one of the important security techniques in cloud storage. In recent years, auditing protocols for cloud storage have attracted much attention and have been researched intensively. These protocols focus on several different aspects of auditing, and how to achieve high bandwidthand computation efficiency is one of the essential concerns. For that purpose, the Homomorphic Linear Authenticator (HLA) technique that supports block less verification is explored to reduce the overheads of computation and communication in auditing protocols, which allows the auditor to verify the integrity of the cloud without retrieving the whole data. The privacy protection of data is also an important aspect of cloud storage auditing. In order to reduce the computational burden ofthe client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to get the client's data after it executes the auditing protocol.

Auditing protocols in are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations.Auditing protocols in can also support dynamic data operations. Other aspects, such as proxy auditing, user revocation and eliminating certificate management in cloud storage auditinghave also been studied. Though many research works about cloudstorage auditing have been done in recent years, a critical securityproblem the key exposure problem for cloud storage auditing, hasremained unexplored in previous researches While all existing protocols focus on the faults or dishonesty of the cloud, they haveoverlooked the possible weak sense of security and/or low security settings at the client.

2. SYSTEM ARCHITECTURE.

System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description isa formal description of a system, organized in a way that supportsreasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed.

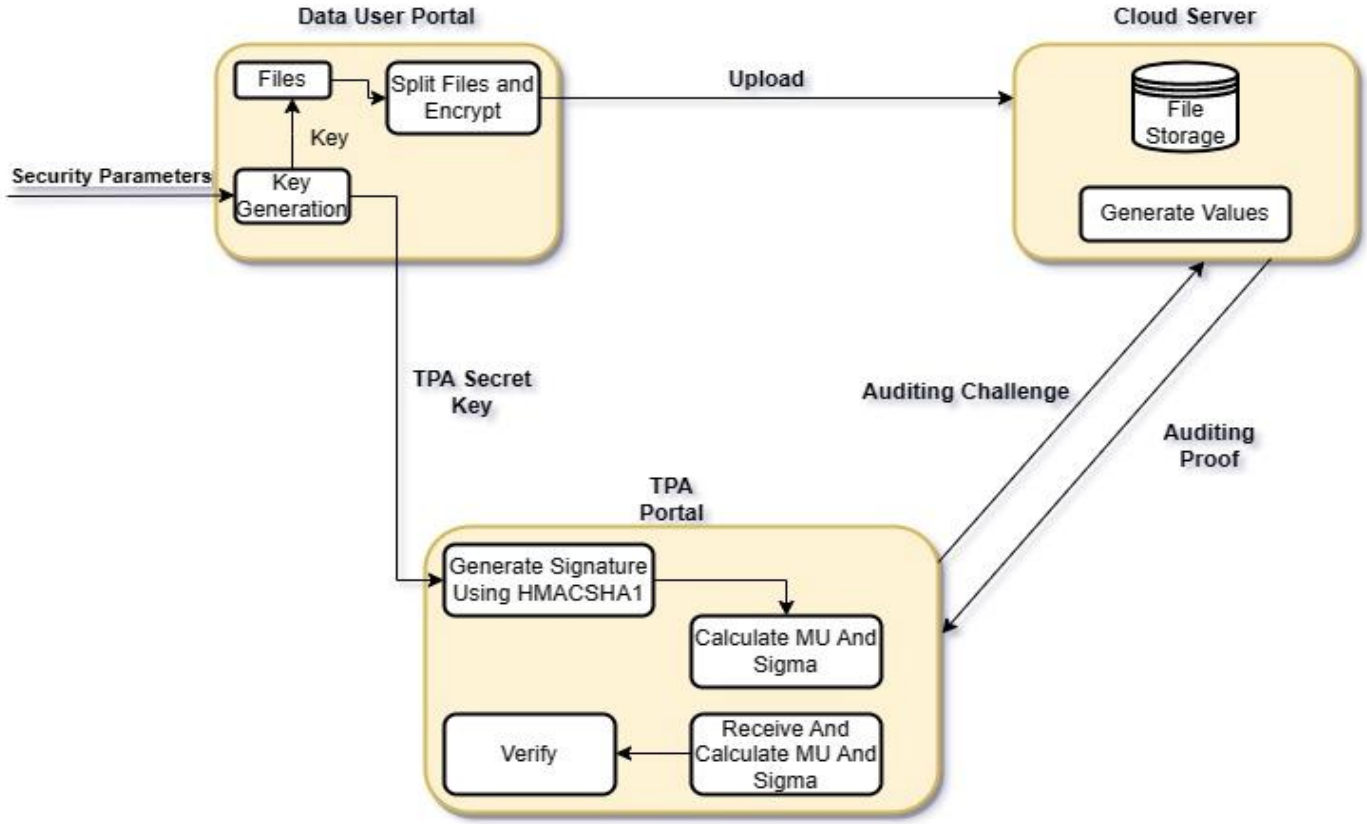

Fig 2.1: System Architecture

2.1 MODULES

Data User
Third Party Auditor
Cloud Server

The above-mentioned modules have following properties.

Key Generation: In this Module public key is generated for authentication for the user to provide the user specificationlogging. The secret key is the confidential generated for eachcandidate during registration.

Auditor Public Key: The auditor public key is generated to perform all the operation with a single key on all the modules. **Proof verification:** the user will verify the files down loaded from data base by using the signatures.

Signature generation: by using primary and secrete key user will store the files in the data base by signature generation using HMACSHA1.

Encrypted security: the user performs encryption on databefore storing the files on the cloud for security purpose.

Key Space: key space refers to the set of all possible keys thatcan be used to generate a key.

PKG: It is responsible for generating system's global parameter,and private keys for *DO* and *DC*.

Data owner: The *DO* uses a mobile device to access or sendencrypted data. Once this action has been performed successfully, the *CC* can store the encrypted data with keywordin the cloud storage space.

Data consumer: The *DO*, who obtains his/her private key from the *PKG*, allowed to perform the decryption process over the encrypted data.

Cloud controller: It is responsible for data processing, such as data computation and storing on behalf of the cloud users.

These entities perform some tasks based on their requirements. First, user (DO and DC) registers himself/herself through a mobile device.

In order to store some data in the cloud, the DO needs to login and performs a mutual authentication between the mobile deviceand the CC. Once it is completed, the DO is able to undertake secure (end-to-end) transactions (e.g., uploading and downloading of data

that has been encrypted using relevant keywords). Any registered user, who act as a DC, wishes to access the stored data will need to login and submit a query to the CC. Only after a successful login, the CC sends the encrypted data to the DC.

In order to decrypt, DC contacts the PKG and receives a privatekey associated with its unique identity, and then proceeds to decrypt the encrypted data using that private key.

3. CLASS DIAGRAM

A class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes.

The class diagram has the following classes:

Main: This class has operations called upload file, downloadfile and audit file.

TPA: This class has operation called Set master key, upload fileto cloud, encrypt file block, decrypt file block and audit file.

Cloud Manager: This class has operation such as store fileblocks, get audit signature and get file blocks.

Block Splitter: this class has operations called split block andreassemble block.

Key Manager: this class has operations called generate sub keyand get keys,

Sign store: This class has operations called store signature andverify signature.

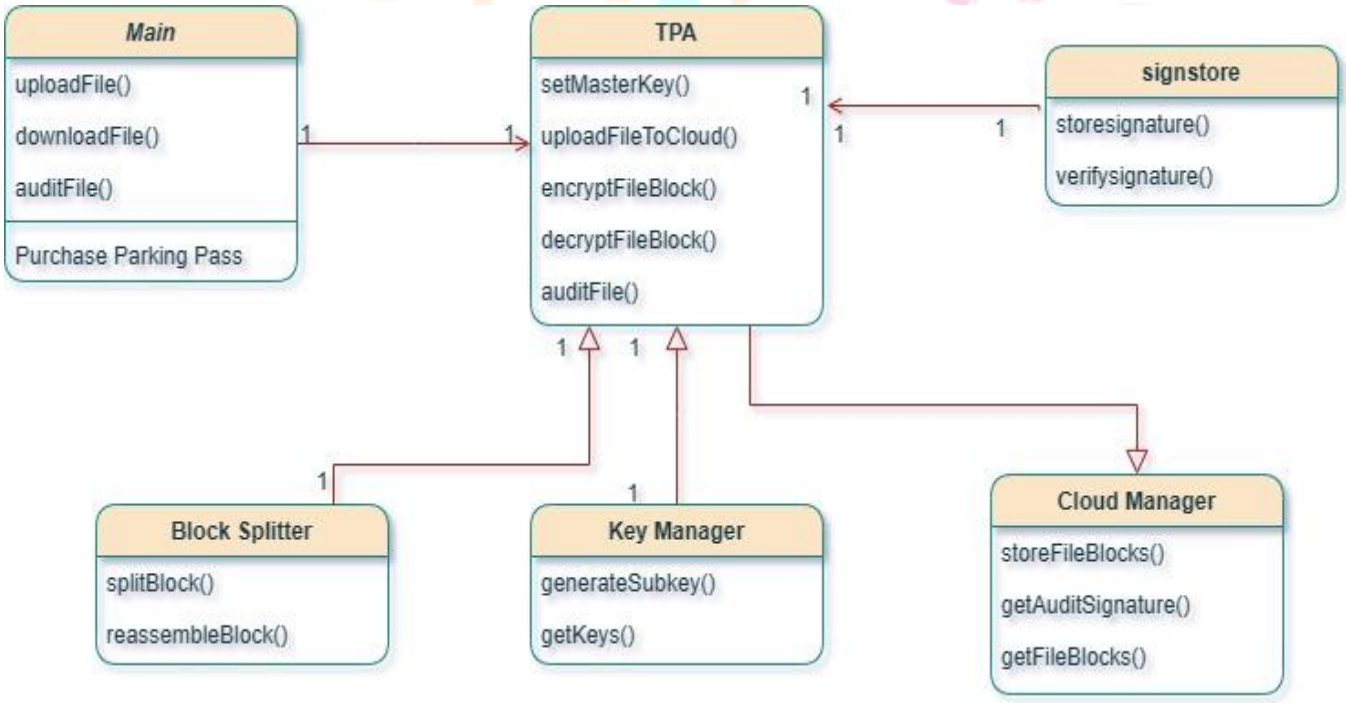

Fig 3.1: Class Diagram

4. SEQUENCE DIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. It is a construct of a Message Sequence Chart.

It helps in envisioning several dynamic scenarios. It portrays the communication between any two lifelines as a time-ordered sequence of events, such that these lifelines took part at the run time. In UML, the lifeline is represented by a vertical bar, whereas the message flow is represented by a vertical dotted line that extends across the bottom of the page. It incorporates the iterations as well as branching.

Sequence Diagram for uploading and splitting Flow

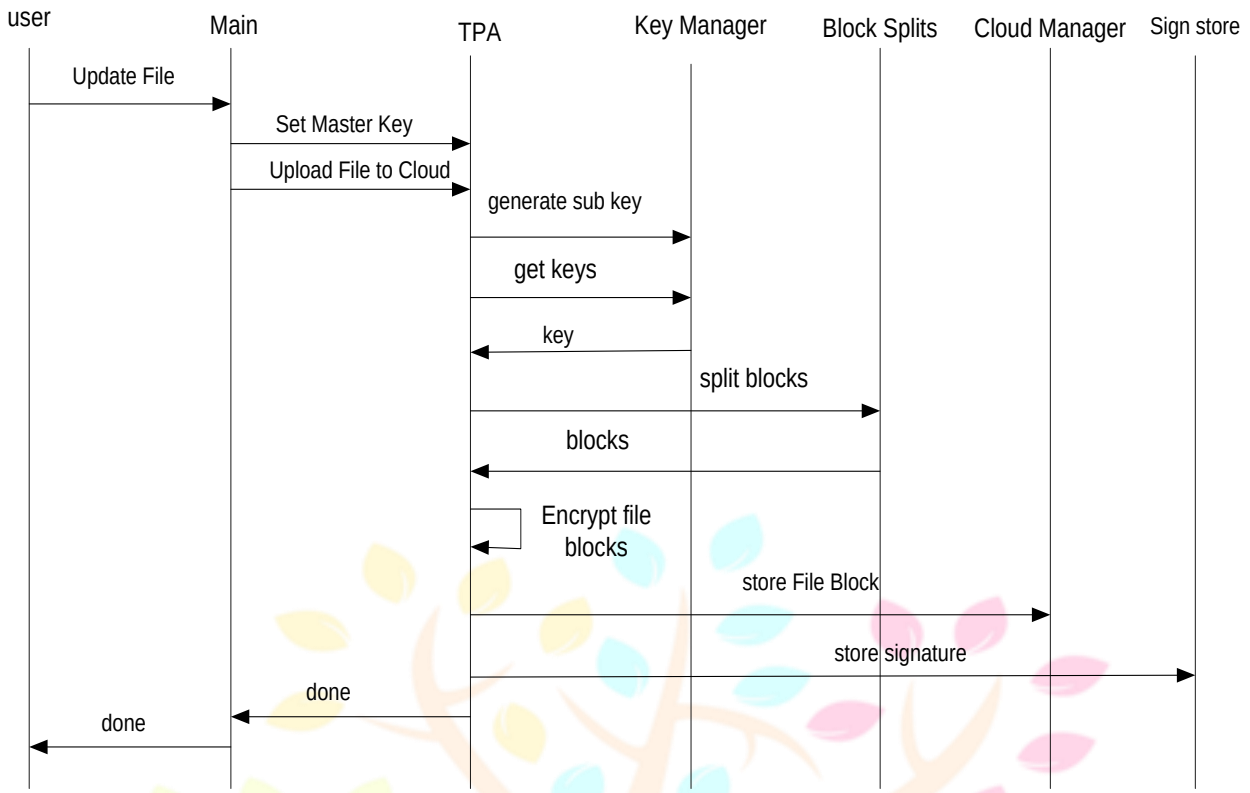

Fig 4.1: Sequence Diagram

Here User, main, TPA, key manager, block splits, cloud managerand sign store are Objects. Each object interacts with other objects in a sequential order through messages. As shown above.

5. SECURITY ANALYSIS

Theorem 1. *The proposed IBE scheme is fair and consistent, inthe sense that for a valid ciphertext generated by any registered client device, the decryption algorithm run by an- other registered client device computes and obtains the correct plaintext.*

Proof: In order to obtain the correct plaintext for user *i*,the decryption algorithm proceeds with $CT = C, T, MD$ using the private key $SK_i = g^r \bmod p$ as follows:

$$Z = e(T_i, SK_i)$$

$$= e\left(g^{ID_i} h\right)^{s}, g^{\frac{\alpha}{\beta+ID_i}}$$

$$= e\left(g^{ID_i} \cdot g^{\beta}\right)^{s}, g^{\frac{\alpha}{\beta+ID_i}}$$

$$= e(g, g)^{\alpha s}$$

Now it computes and checks

$$LHS = M = \left(C_{c'}^{'} \cdot Z\right) \bmod p$$

$$= \left(C_2^{'} \bmod p\right) \cdot e(g, g)^{\alpha s}$$

$$= M \cdot Y 1_{s_2}^{-1} \bmod p \cdot e(g, g)^{\alpha s} \bmod p$$

$$= \left(M \cdot Y 1 \cdot e(g, g)^{\alpha s}\right) \bmod p$$

$$= M \cdot e(g, g)^{-\alpha s} \cdot e(g, g)^{\alpha s} \bmod p$$

$$= M = RHS$$

where $T_i \in T$ and $s'_2 = s_2 = H(Y 1' \| T) = H(Y 1' \| T)$.

Thus, it computes MD = H $(ID_S M')\|$ and returns the correct plaintext *M* as output. Similarly, it satisfies case 2(for group communication) in the *IBE. Decrypt* algorithm.

This completes the IBE scheme

Theorem 2. *The proposed IBADS protocol is semanticallysecure, i.e., an unregistered client device cannot retrieve any information about the message.*

Proof: The proof of this theorem follows when Lemmas 2.1 is satisfied.

Lemma 2.1. *The proposed authentication technique in IBADS is secure against known security attacks such as insider, impersonation and session key computation attacks, and provides users' anonymity.* Thus, it computes $MD = H(ID_S \quad M')$ and returns the correct plaintext M as output.
Similarly, it satisfies case 2(for group communication)in the *IBE. Decrypt* algorithm.
This completes the IBE scheme. The whole processes inthe proposed IBADS protocol discussed in Section III-A is presented in Figures 3 and 4.

6. RELATED WORK

Extensive security and performance analysis show the proposedschemes are provably secure and highly efficient. Using CloudStorage, users can remotely store their data and enjoy the on- demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage isof critical importance so that users can resort to a third-partyauditor(TPA) to check the integrity of outsourced data and be worry-free.To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocolinto a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensiveanalysis shows that our schemes are provably secure and highlyefficient.

To achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication.
To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature toextend our main result into a multi-user setting, where TPA canperform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposedscheme is highly efficient and provably secure. To ensure clouddata storage security, it is critical to enable a third-party auditor(TPA) to evaluate the service quality from an objective and independent perspective. Public auditability also allows clientsto delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is how to construct verification protocols that can accommodate dynamic data files. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support ofeither public auditability or dynamic data operations, this paper achieves both.

Experimental results show that the cloud can improve theefficiency of user revocation, and existing users in the group can save a significant amount of computation andcommunication resources during user revocation. With data services in the cloud, users can easily modify and share data asa group. To ensure data integrity can be audited publicly, usersneed to compute signatures on all the blocks in shared data. Different blocks are signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks, which were previously signed by this revoked user, must be re-signed by an existing user. The straightforward method, whichallows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrityof shared data with efficient user revocation in mind. By utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so thatexisting users do not need to download and re-sign blocks by themselves.

In addition, a public verifier is always able to audit the integrityof shared data without retrieving the entire data from the cloud,even if some part of shared data has been re-signed by the cloud.Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

Cryptographic computations are often carried out on insecure devices for which the threat of key exposure represents a serious and realistic concern. In an effort to mitigate the damagecaused by exposure of secret keys stored on such devices, the paradigm of forward security was introduced. In a forward-securescheme, secret keys are updated at regular periods of time; exposure of the secret key corresponding to a given time period does not enable an adversary to "break" the scheme (in the appropriate sense) for any prior time period. A number of constructions of forward-secure digital signature schemes, key- exchange protocols, and symmetric-key schemes are known. Author presents the first non-trivial constructions of (non- interactive) forward-secure public-key encryption schemes. Our main construction achieves security against chosen-plaintext attacks under the decisional bilinear Diffie-Hellman assumption inthe standard model. This scheme is practical, and all parameters grow at most logarithmically with the total number of time periods.We also give a slightly more efficient scheme in the random oraclemodel. Both our schemes can be extended to achieve security against chosen-cipher text attacks and to support an unbounded number of time periods.

7. RESULTS

Fig7.1: Cloud Server

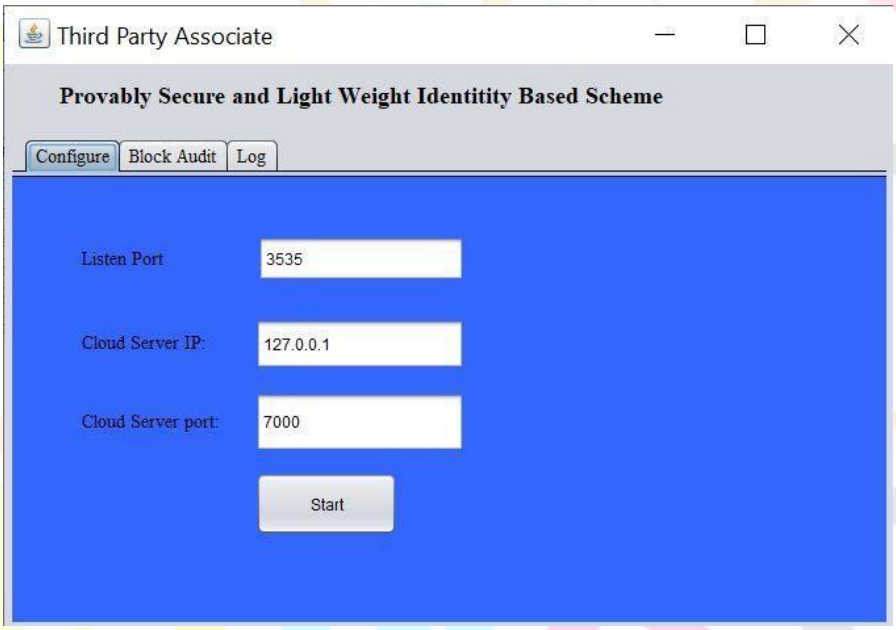

Fig7.2: Third Party Auditor

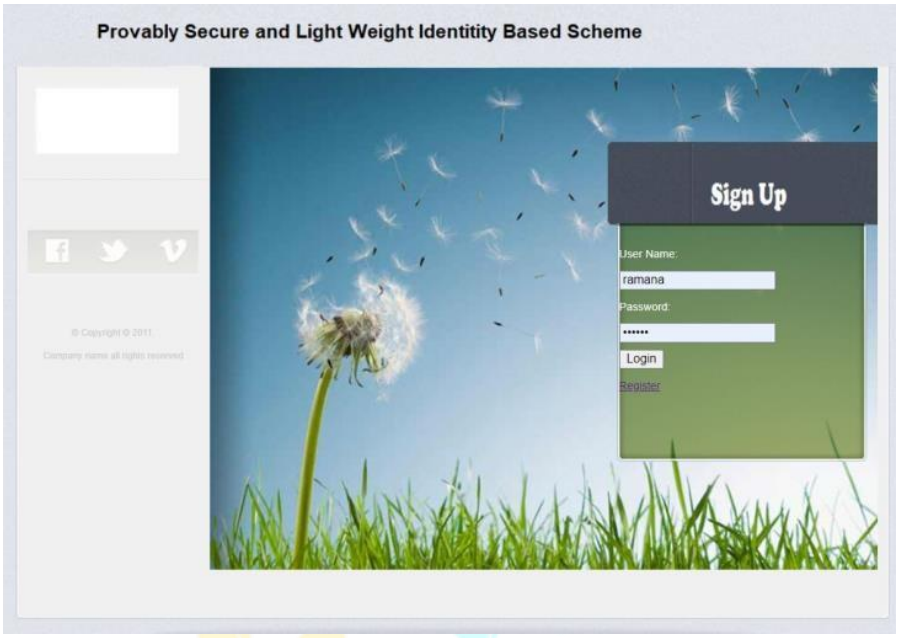

Fig7.3: User Interface

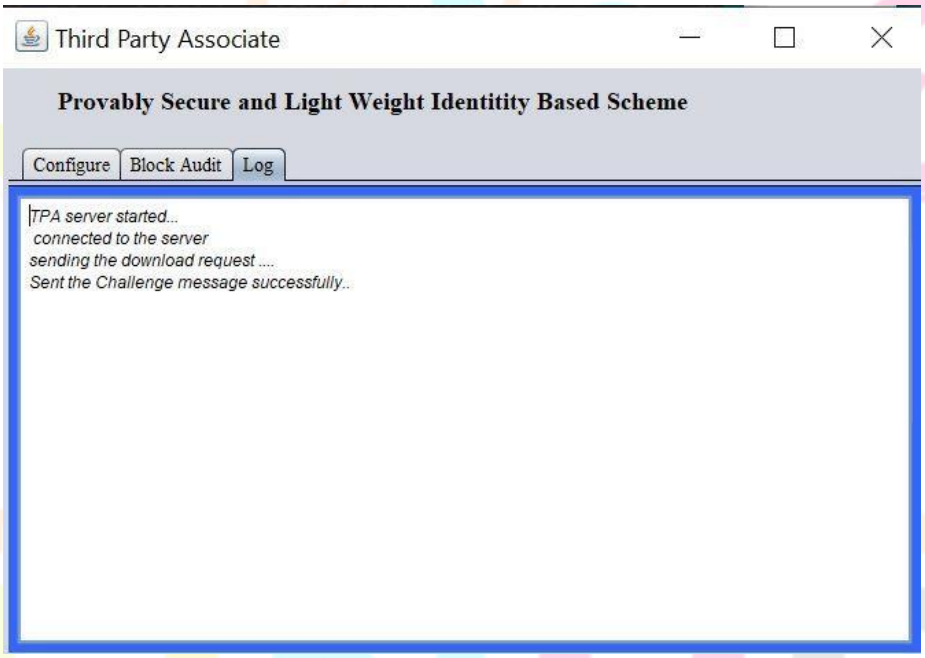

Fig7.4: Establishing Connection with Cloud

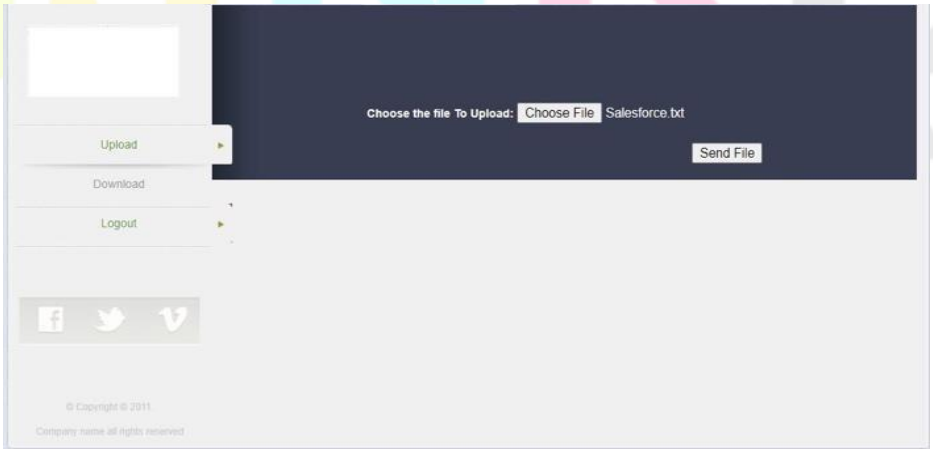

Fig7.5: File upload Interface

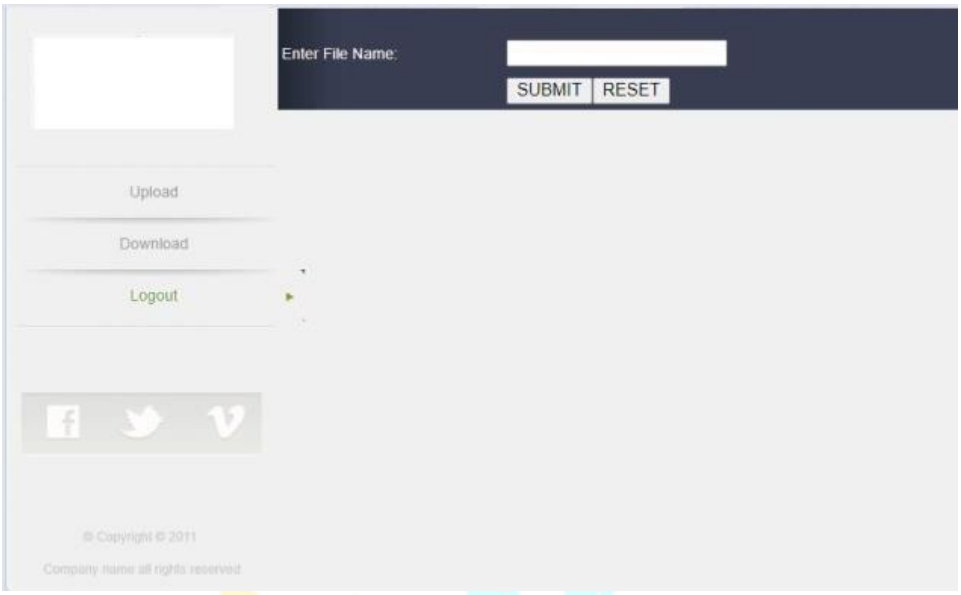

Fig 7.6: File download Interface

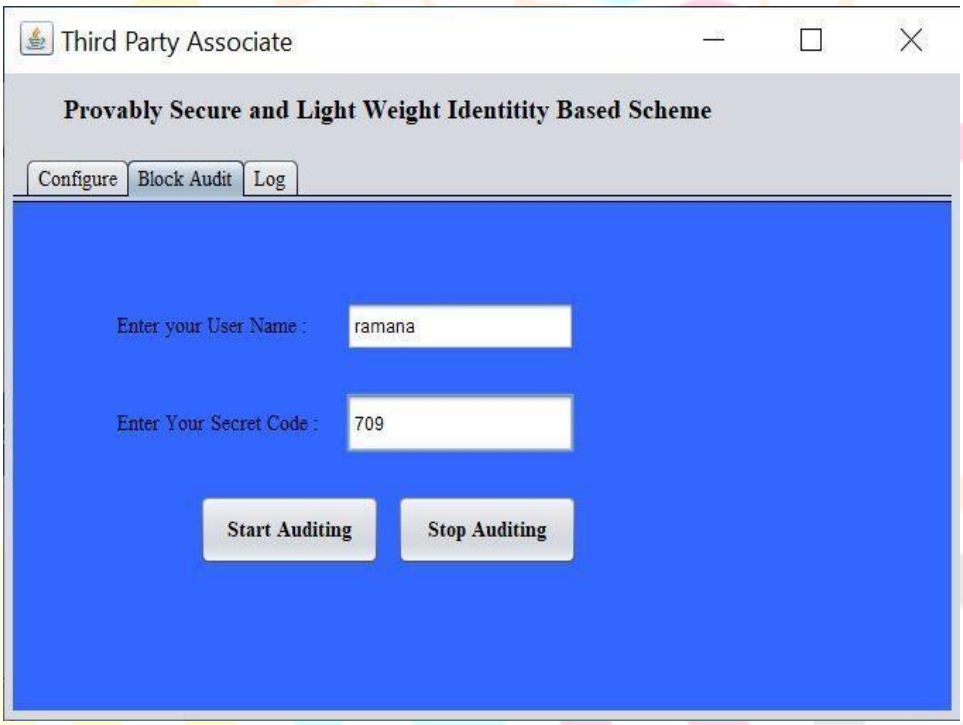

Fig 7.7: Auditing files

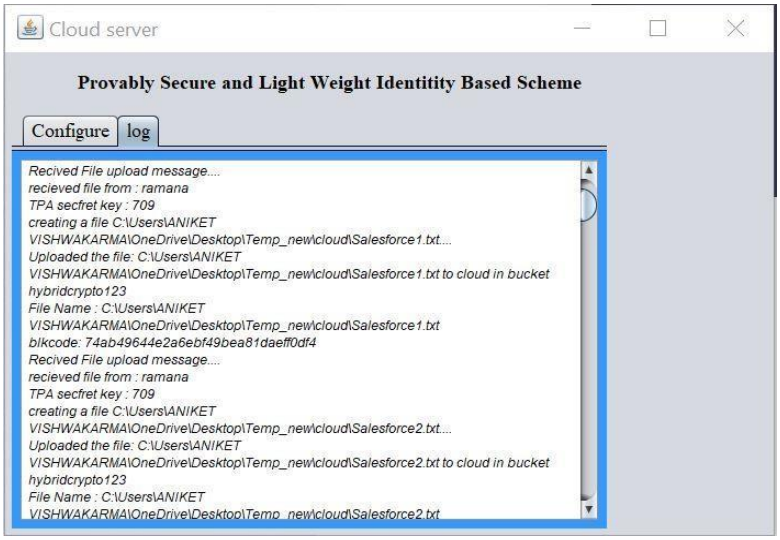

Fig 7.8: Cloud Log

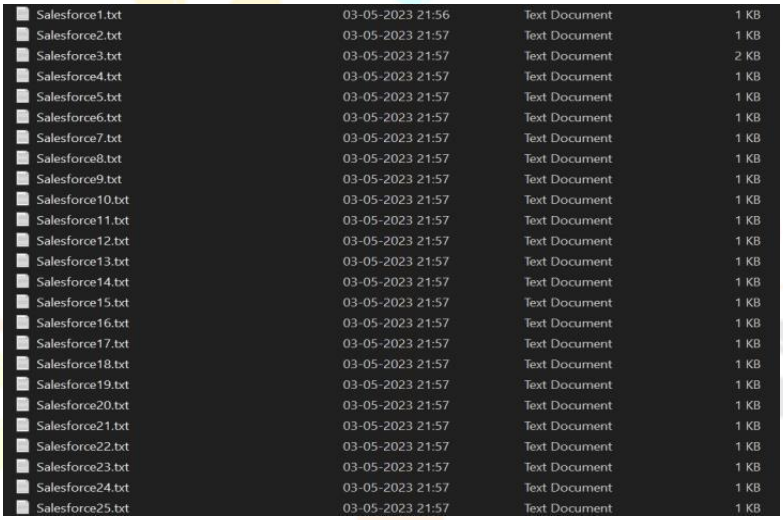

Fig 7.9: Split Files

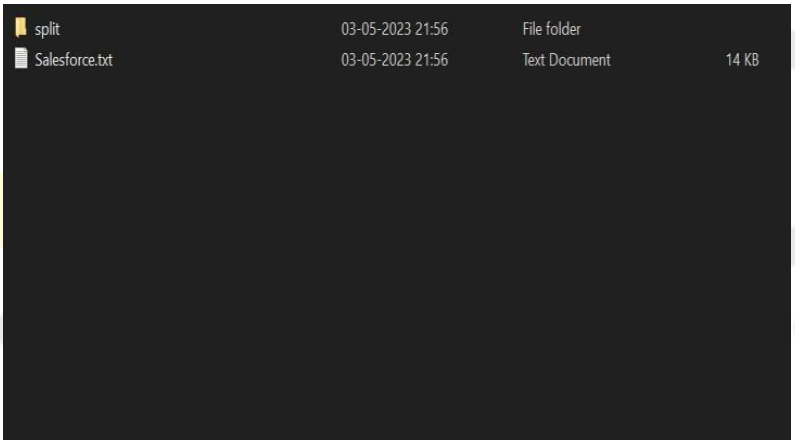

Fig 7.10: Downloaded Files

8. CONCLUSION

The Secure Identity-Based Authenticated Data Sharing Protocol is a critical aspect of Cyber-Physical Cloud security. The implementation of this protocol can help to ensure the security of sensitive data in the cloud environment. This protocol provides an efficient and secure data sharing mechanism among cloud users. It eliminates the need for digital certificates and simplifies key management. It also provides access control mechanisms to ensure that only authorized users can access sensitive data. A new identity- based authenticated data sharing (IBADS) protocol is designedfor cyber-physical cloud systems based on bilinear pairing in the IBADS, there are two phases. First, a new data owner needs to register. Second, the data owner sends an encrypted message to the trusted cloud controller using the client devices. The system then portrays the security and correctness of the protocol, as well as evaluating its performance.

9. REFERENCES

[1] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No.9, pp. 1717-1726, 2013.

[2] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362- 375, 2013.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "En- abling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[4] B. Wang, B. Li, and H. Li. "Public auditing for shared data with efficient user revocation in the cloud," INFO- COM 2013 Proceedings IEEE, pp. 2904-2912, 2013.

[5] F. Hu, C.H. Wu and J.D. Irwin, "A new forward secure signature scheme using bilinear maps," Cryptology ePrint Archive, Report 2003/188, 2003.

[6] Jiafu Wan, Hehua Yan, Di Li, Keliang Zhou, and Lu Zeng. Cyber- physical systems for optimal energy management scheme of autonomouselectric vehicle. *TheComputer Journal*, 56(8):947–956, 2013.

[7] Ragunathan Rajkumar. A cyber–physical future.*Proceedings of the IEEE*, 100(Special Centennial Issue):1309– 1312, 2012.

[8] Akshay Rajhans, Ajinkya Bhave, Ivan Ruchkin, Bruce H Krogh, David Garlan, Andre´ Platzer, and Bradley Schmerl. Supporting heterogeneity in cyber-physical systems architectures. *IEEE Transactions on Automatic Control*, 59(12):3178–3193, 2014.

[9] Burak Demirel, Zhenhua Zou, Pablo Soldati, and Mikael Johansson. Modular design of jointly optimal controllers and forwarding policies forwireless control. *IEEE Transactions onAutomatic Control*, 59(12):3252–3265, 2014.

[10] Zhaogang Shu, Jiafu Wan, Daqiang Zhang, and Di Li. Cloud-integrated cyber-physical systems for complex industrial applications. *Mobile Networks and Applications*, 21(5):865–878, 2016.

[11] I NARSIMHA RAO, M SUPRIYA MENON, and SVIVEKA. Cloud based secure health care system using multi authority. 2015.