Novel Method to Achieve Data Integrity Auditing In Cloud Server

MANDELA MANJU [#1], B.SURYANARAYANA MURTHY [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Associate Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

In current day's cloud computing has become one of the fascinating domains which are used by almost all MNC and IT companies.Using cloud storage services, 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. They require a physical device to authenticate the identity by using third party devices like smart card or some token generators. If this token generator or smart card is lost or this password is forgotten, most of the current data integrity auditing schemes would be unable to work. In order to overcome this problem, we propose a new 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) as the user's fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

1. INTRODUCTION

CLOUD storage can provide powerful and on-demand data storage services for users [1]. By using the cloud service, users can outsource their data to the cloud without wasting substantial maintenance expenditure of hardware and 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 private key. A feasible method is to use biometric data, such as fingerprint and iris scan [16, 17], as the private key. Biometric data, as a part of human body, can uniquely link the individual and the private key. Unfortunately, biometric data is measured with inevitable noise each time and cannot be reproduced precisely [18] 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 so on. Therefore, the biometric data cannot be used directly as the private key to generate authenticators in data integrity auditing. Contribution.

How to 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 named as MBLSS by modifying the BLS short signature based on the idea of fuzzy signature. We give the security analysis and justify the performance via concrete implementations. The results show that the proposed scheme is secure and efficient.

PROBLEM STATEMENT

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.

PURPOSE

The contribution of this paper can be summarized as follows: We initiate the first study on how to employ biometric data as fuzzy private key to perform data integrity auditing, and propose a new paradigm called data integrity auditing without private key storage. In such a scheme, a user utilizes biometric data as his fuzzy private key for confirming his identity. The data integrity auditing can be performed under the condition that there is not any hardware token for storing the private key. We further formalize the definition of data integrity auditing scheme without private key storage for secure cloud storage. We design a practical data integrity auditing scheme without private key storage for secure cloud storage.

OBJECTIVE

We propose a new 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) as the user's fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

The main scope for designing this current application is to overcome the problem which is faced in current networks .In present days there was no security for the data which is stored in the cloud server, because the data is not encrypted by strong means of encryption and there is no facility to block the un-authorized data access.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

1) Public Key Encryption with Keyword Search.

Author: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano.

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

2) VABKS: Verifiable Attribute-Based Keyword Search Over Outsourced Encrypted Data.

Author: Q. Zheng, S. Xu, and G. Ateniese.

It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VA B K S and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

3) Fuzzy identity-based encryption.

Author: A. Sahai and B. Waters.

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

3. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the existing clouds there is no security for the sensitive data which is uploaded into the cloud server.

LIMITATION OF EXISTING SYSTEM

The following are the main limitations of the existing system. They are as follows:

1) In the existing clouds there is no method like revocation identification in the cloud server.

2) All the data is accessed by centralized server and hence if the hacker or intruder hack the centralized location, then he/she can access or modify any users data that is available in the server.

3) The traditional account/password-based authentication is not privacy preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems.

4. PROPOSED SYSTEM

We propose a new 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) as the user's fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system, they are as follows:

1) The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

2) The performance comparisons indicate that the proposed protocol has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1) Data Owner
2) Cloud Server
3) TPA
4) Data User

Now let us discuss about each and every module in detail

5.1 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, View Transactions.

5.2 CLOUD SERVER

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

5.3 TPA

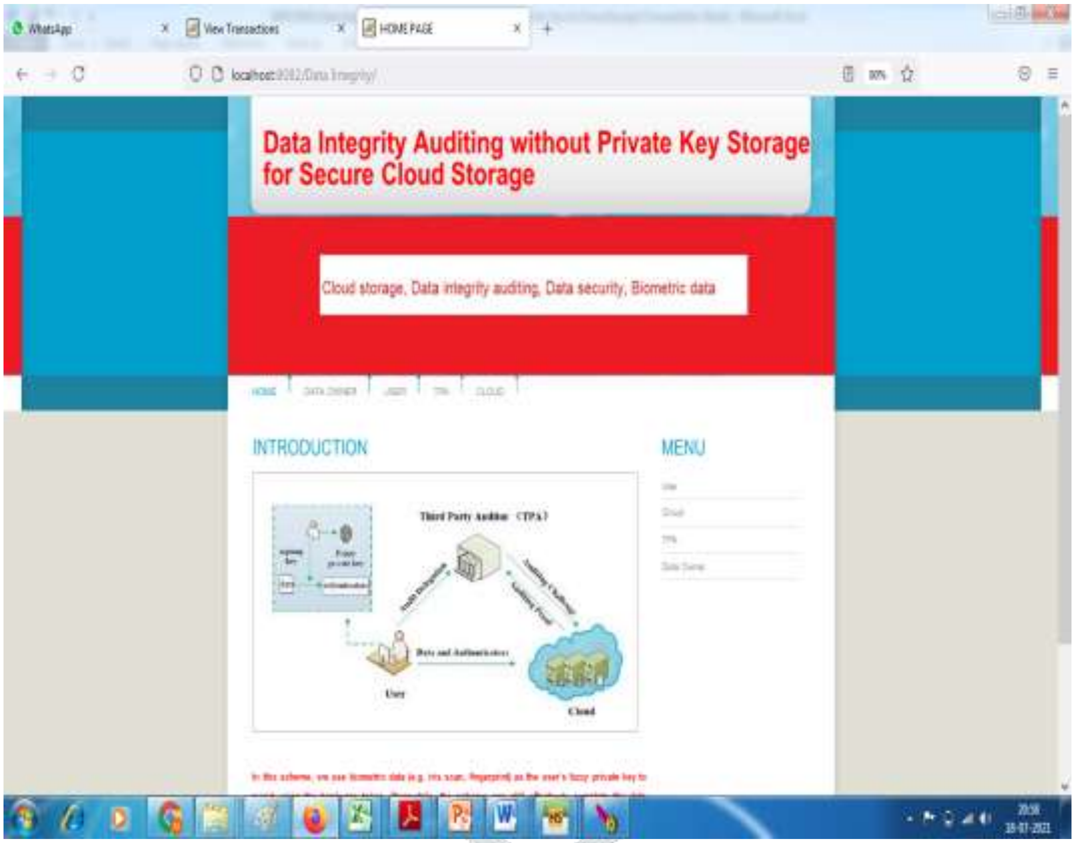
In this module, the TPA performs the following operations such as View Metadata Details, View All Transactions, and View All Attackers

5.4 DATA USER

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

6. RESULTS (OUTPUT SCREENS)

1 Home Page



Data Integrity Auditing without Private Key Storage for Secure Cloud Storage

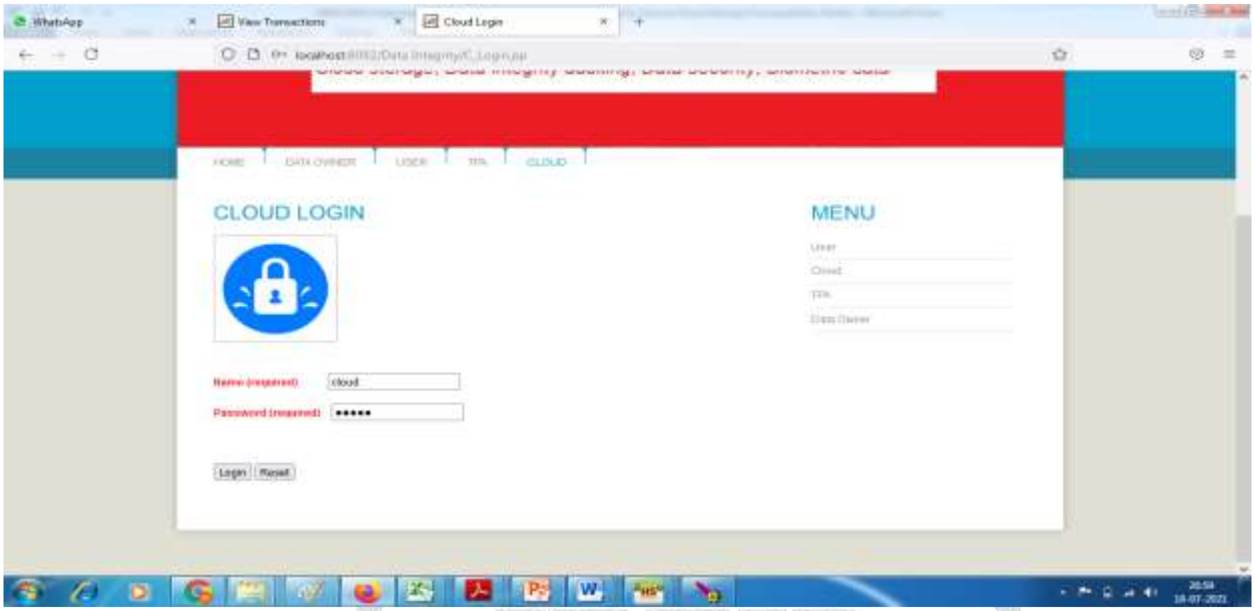
Cloud storage, Data integrity auditing, Data security, Biometric data

In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the user's fuzzy private key to

Explanation:

The home page mainly contains the following links like Data owner, Cloud server, TPA and the End users. All are connected within the same main page.

2) CLOUD SERVER LOGIN



CLOUD LOGIN

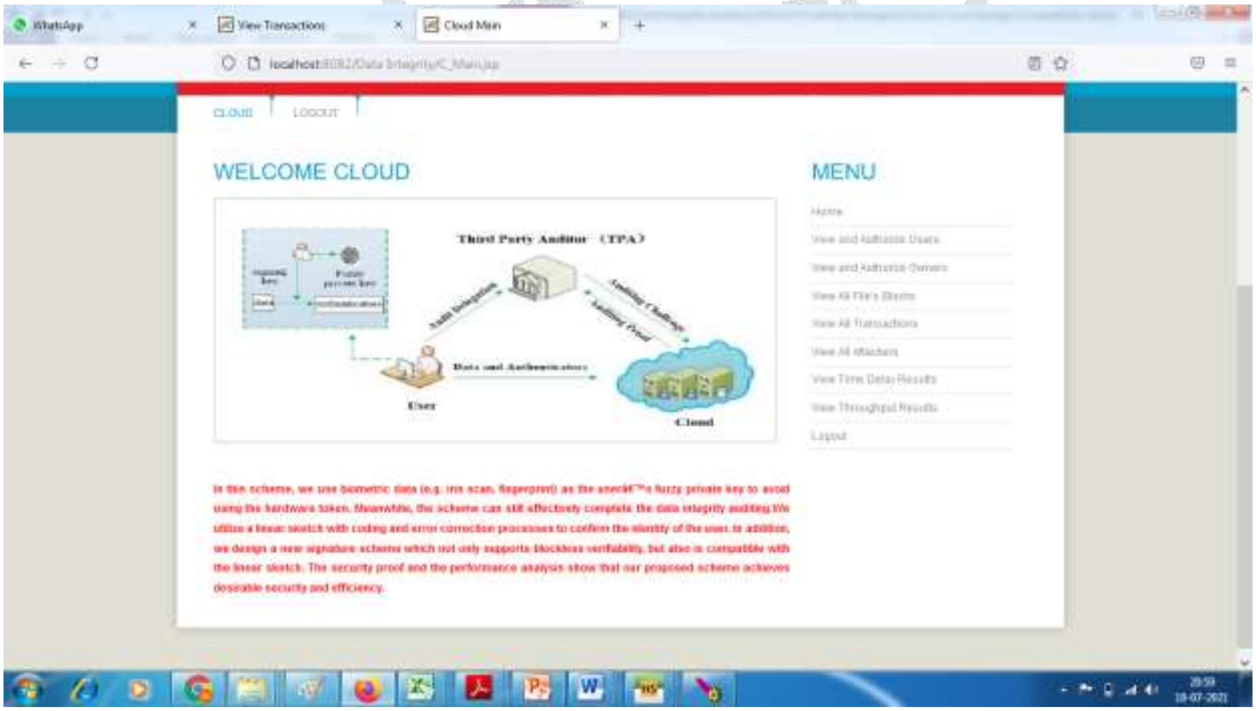
Name (required) cloud

Password (required) •••••

Login Reset

Explanation:

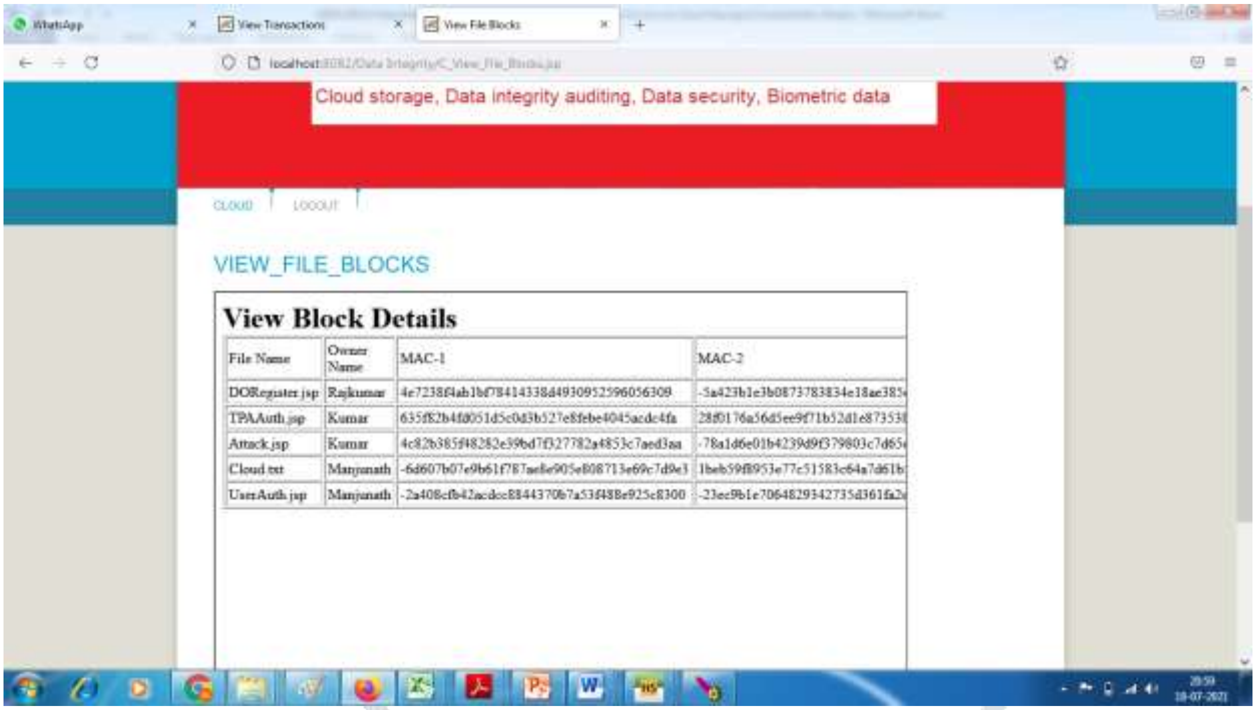
Here the storage server or admin is one who can enter with a valid user name and password and they can verify the following details as follows.



WELCOME CLOUD

In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the userâ€™s fuzzy private key to avoid using the hardware token. Meanwhile, the scheme can still effectively complete the data integrity auditing.We utilize a linear sketch with coding and error correction processes to confirm the identity of the user. In addition, we design a new signature scheme which not only supports blockless verifiability, but also is compatible with the linear sketch. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

3) Cloud server can view the list of all files that are uploaded in the storage server

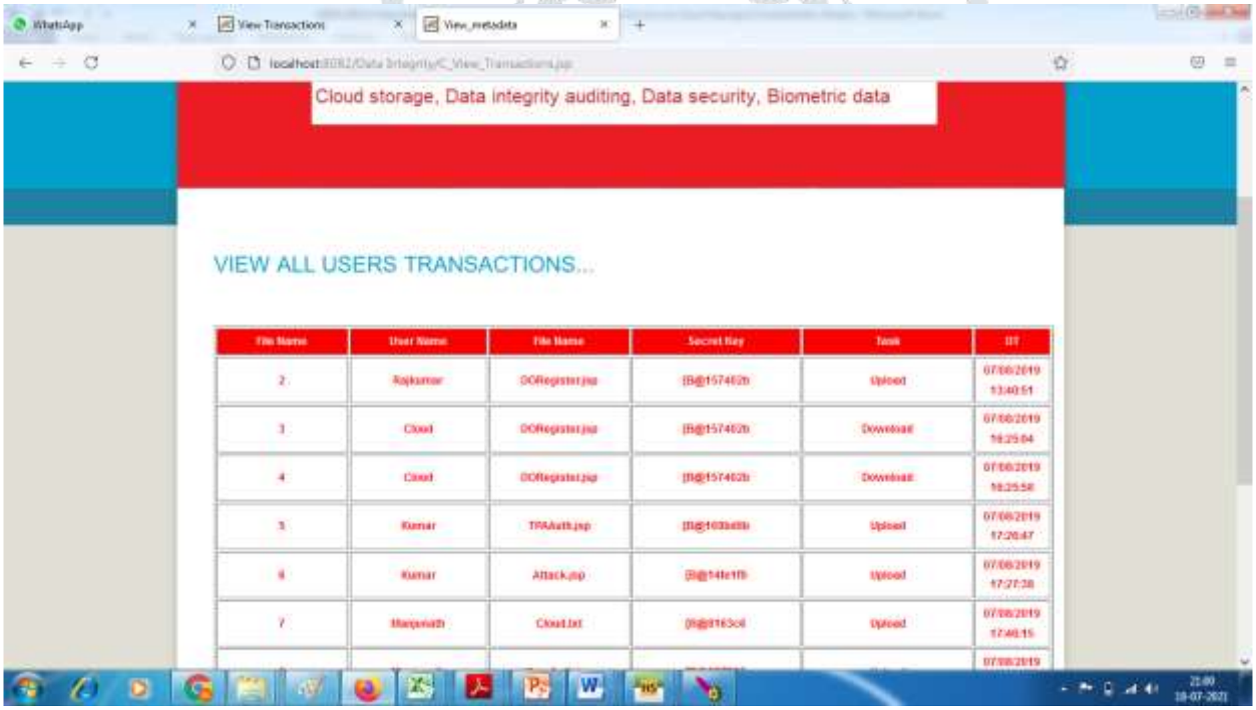

WhatsApp
View Transactions
View File Blocks
localhost:8082/Data Integrity/C_View_File_Blocks.jsp
Cloud storage, Data integrity auditing, Data security, Biometric data
CLOUD
LOGOUT

VIEW_FILE_BLOCKS

View Block Details

File Name	Owner Name	MAC-1	MAC-2
DORegister.jsp	Rajkumar	4e7238f4ab1bf78414338d4930952596056309	-5a423b1e3b0873783834e18ae385
TPAAuth.jsp	Kumar	635f82b4fd051d5c0d3b527e8febe4045acdc4fa	28f0176a56d5ee9f71b52d1e87353
Attack.jsp	Kumar	4c82b385f48282e39bd7f327782a4853c7aed3aa	-78a1d6e01b4239d9f379803c7d65
Cloud.txt	Manjunath	-6d607b07e9b61f787ae8e905e808713e69c7d9e3	1beb59f8953e77c51583c64a7d61b
UserAuth.jsp	Manjunath	-2a408cfb42acdce8844370b7a53f488e925c8300	-23ec9b1e7064829342735d361fa2

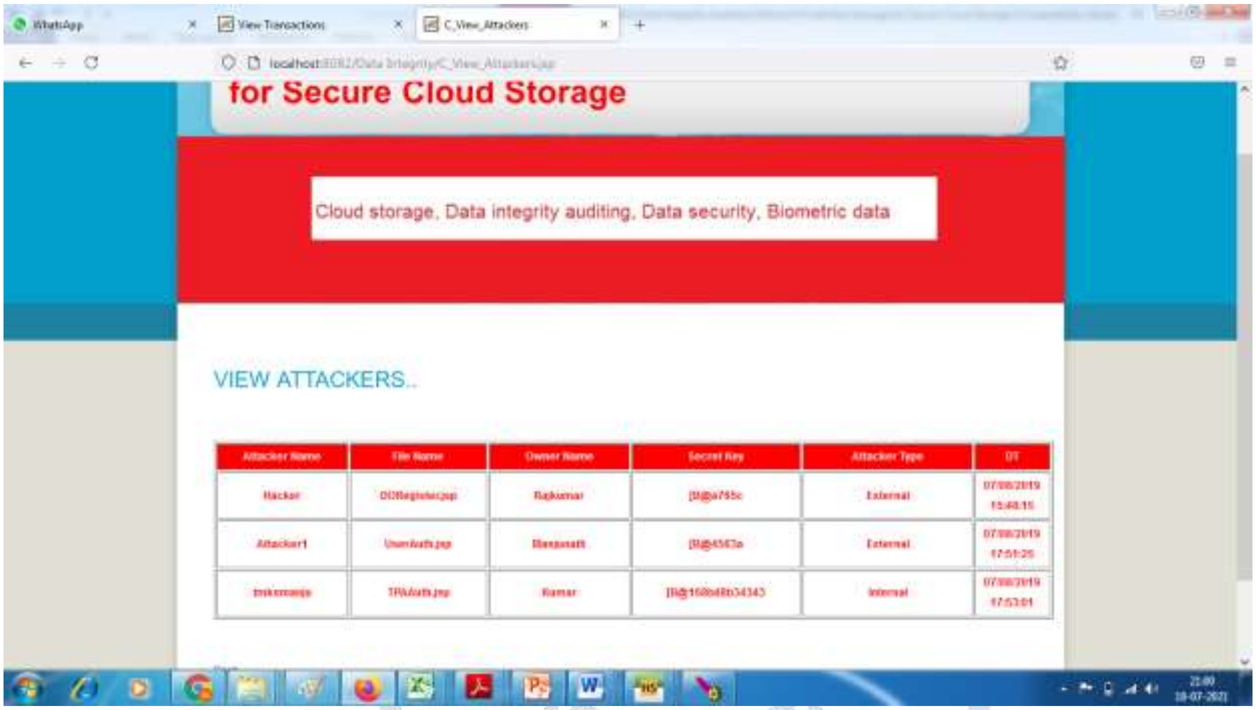
4) Cloud server can view Set of all users transactions


WhatsApp
View Transactions
View_metadata
localhost:8082/Data Integrity/C_View_Transactions.jsp
Cloud storage, Data integrity auditing, Data security, Biometric data

VIEW ALL USERS TRANSACTIONS...

File Name	User Name	File Name	Secret Key	Task	DT
2	Rajkumar	DORegister.jsp	[B@157402b	Upload	07/08/2019 13:40:51
3	Cloud	DORegister.jsp	[B@157402b	Download	07/08/2019 16:25:04
4	Cloud	DORegister.jsp	[B@157402b	Download	07/08/2019 16:25:58
5	Kumar	TPAAuth.jsp	[B@103bd8b	Upload	07/08/2019 17:20:47
6	Kumar	Attack.jsp	[B@14fe1fb	Upload	07/08/2019 17:27:38
7	Manjunath	Cloud.txt	[B@8163cd	Upload	07/08/2019 17:40:15
					07/08/2019

5)Cloud Server can view all the attacker details



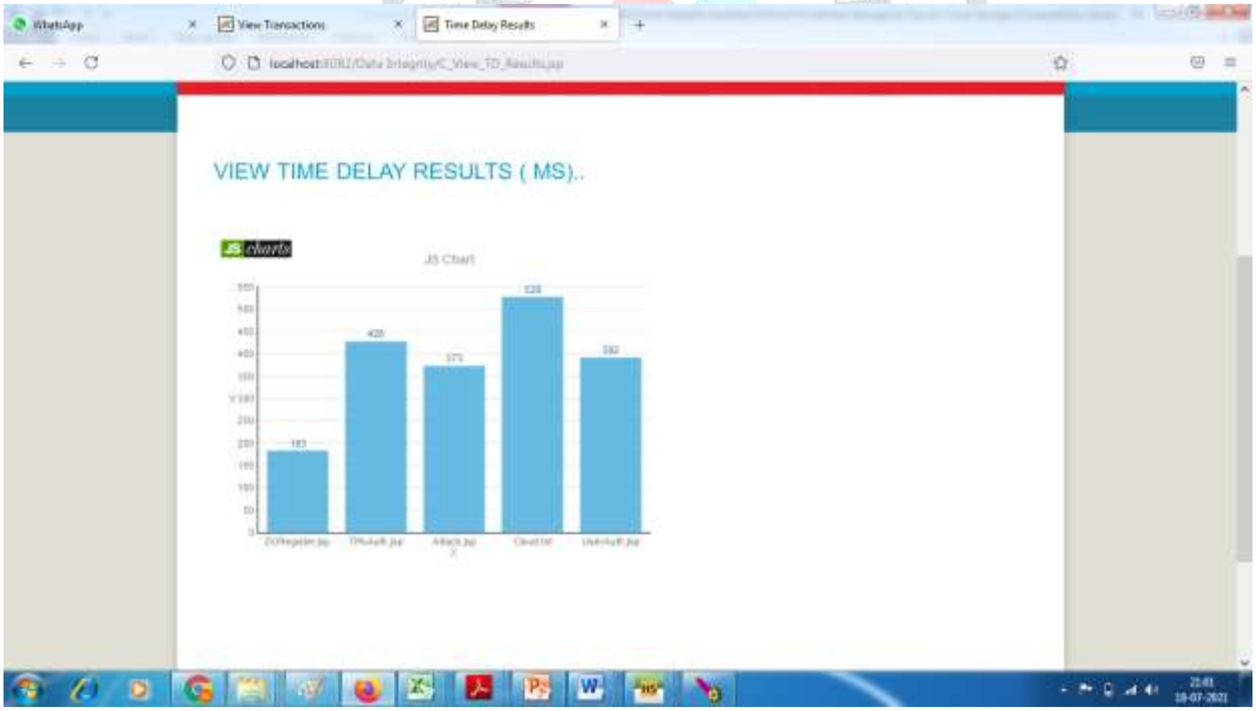
for Secure Cloud Storage

Cloud storage, Data integrity auditing, Data security, Biometric data

VIEW ATTACKERS..

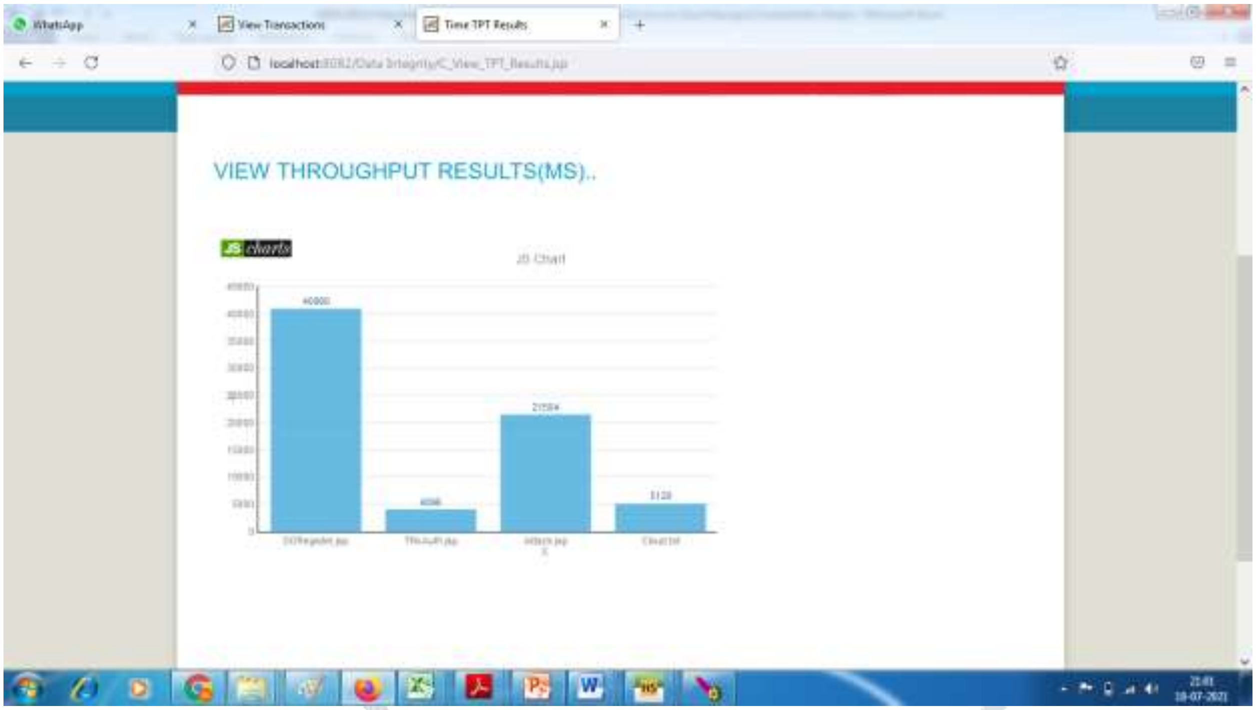
Attacker Name	File Name	Owner Name	Secret Key	Attacker Type	DT
Hacker	DORegister.jsp	Rajkumar	[B@a765c	External	07/08/2019 15:48:15
Attacker1	UserAuth.jsp	Manjunath	[B@4567a	External	07/08/2019 17:51:25
tmksmanju	TPAAuth.jsp	Kumar	[B@1686d8b34343	Internal	07/08/2019 17:53:01

6)Cloud Server can view Time Delay Result



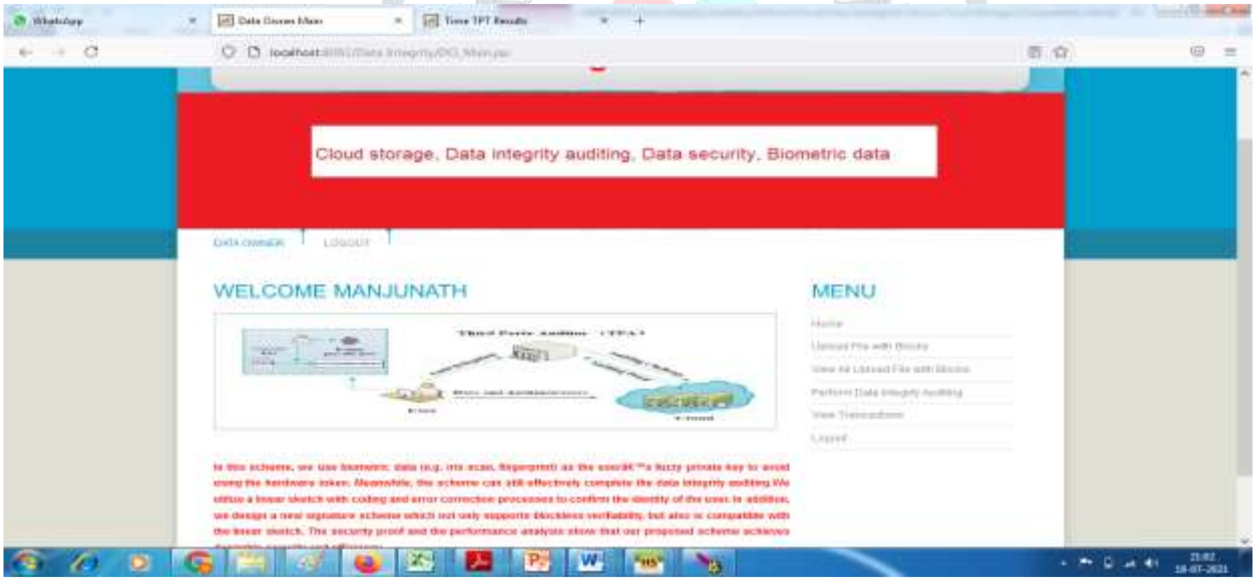
VIEW TIME DELAY RESULTS (MS)..

7)Cloud Server can view the Throughput Details



VIEW THROUGHPUT RESULTS(MS)..

8)User Login

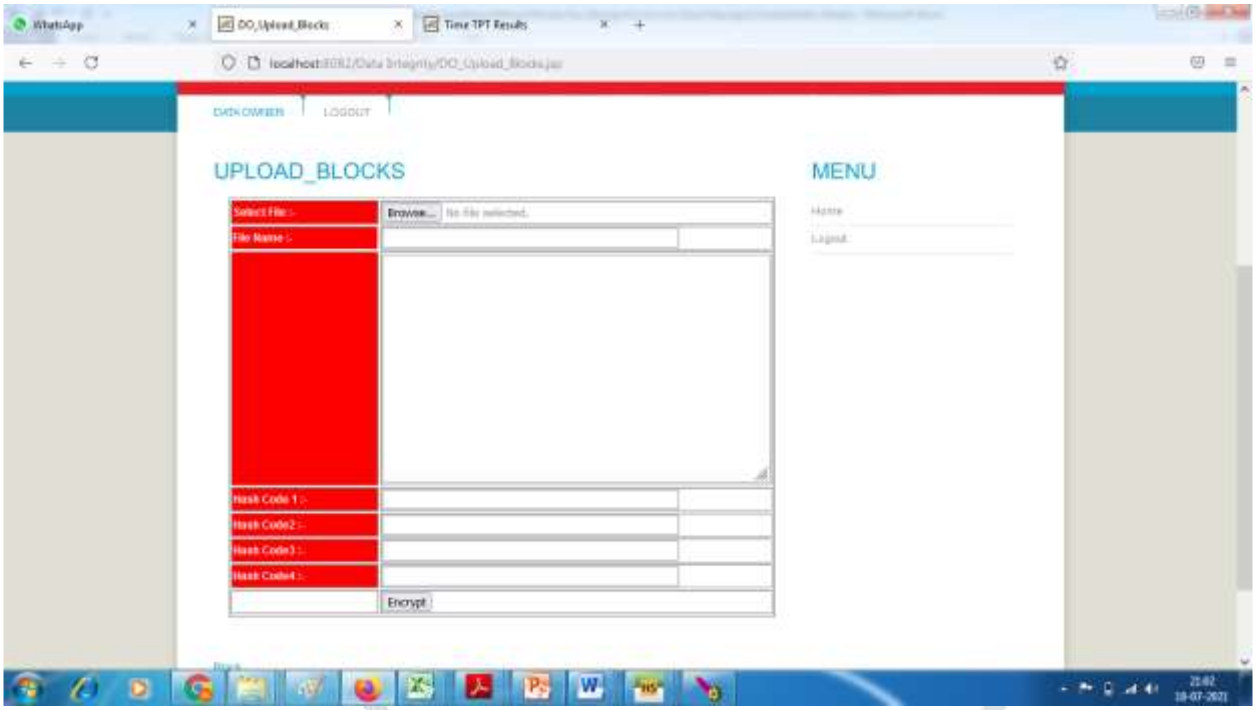


Cloud storage, Data integrity auditing, Data security, Biometric data

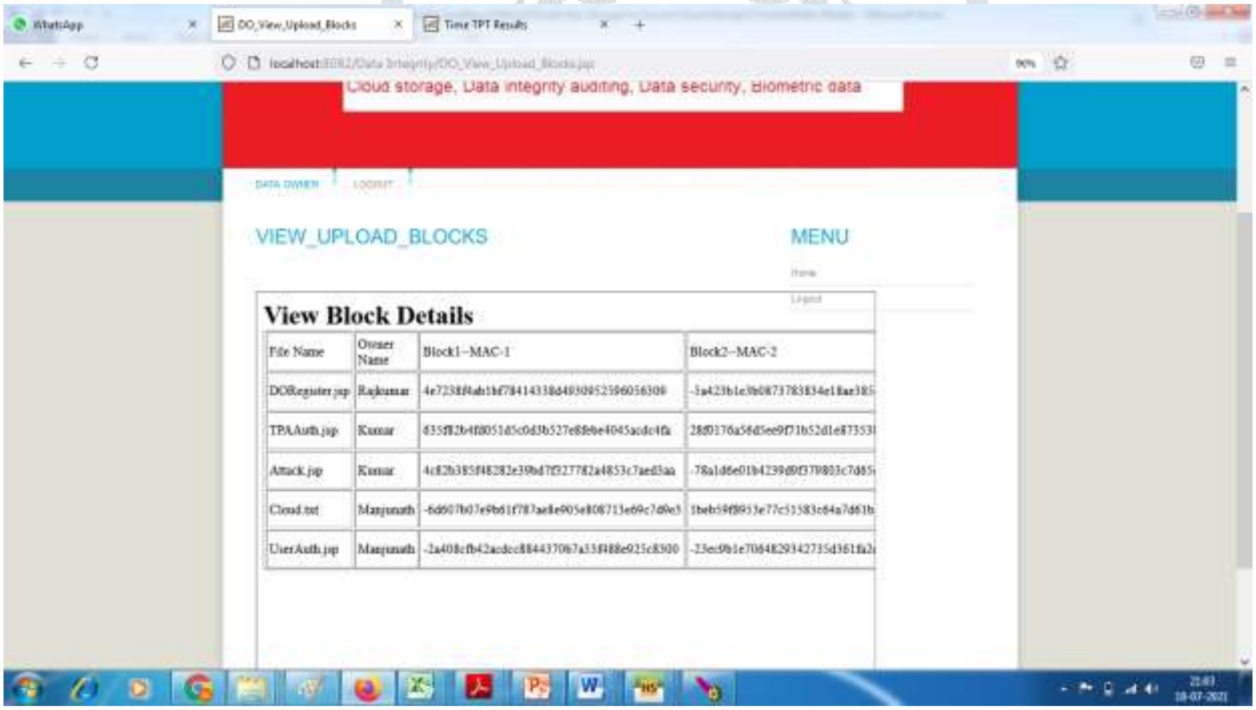
WELCOME MANJUNATH

In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the userâ€™s fuzzy private key to avoid using the hardware token. Meanwhile, the scheme can still effectively complete the data integrity auditing.We utilize a linear sketch with coding and error correction processes to confirm the identity of the user. In addition, we design a new signature scheme which not only supports blockless verifiability, but also is compatible with the linear sketch. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

9)User Can upload a file

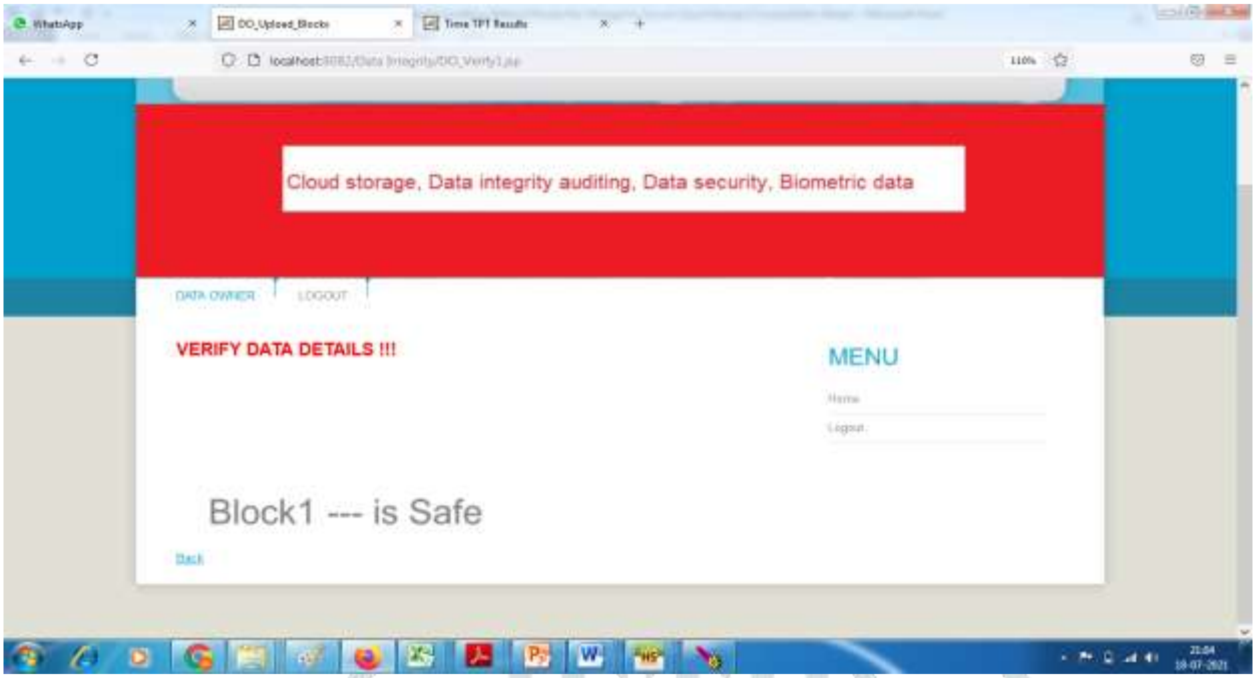


10)User can View all the File Blocks


WhatsApp
DO_View_Upload_Blocks
Time TPT Results
localhost:8082/Data Integrity/DO_View_Upload_Blocks.jsp
Cloud storage, Data integrity auditing, Data security, Biometric data
DATA OWNER
LOGOUT
VIEW_UPLOAD_BLOCKS
MENU
Home
Logout

View Block Details

File Name	Owner Name	Block1--MAC-1	Block2--MAC-2
DORegister.jsp	Rajkumar	4e7238f4ab1bf78414338d4930952596056308	-5a423b1e3b0873783834e1fae385
TPAAuth.jsp	Kumar	d35f82b4f8051d5c0d3b527e8febe4045acdc4fa	28f0176a56d5ee9f71b52d1e87353
Attack.jsp	Kumar	4c82b385f48282e39bd7f327782a4853c7aed3aa	-78a1d6e01b4239d9f370803c7d85
Cloud.txt	Manjunath	-6d607b07e9b61f787ae8e905e808713e69c7d9e3	5beb59f8953e77c51583c64a7d61b
UserAuth.jsp	Manjunath	-2a408cfb42acdec8844370b7a33f488e925c8300	-23ec9b1e7084829342735d361fa2


Cloud storage, Data integrity auditing, Data security, Biometric data
DATA OWNER
LOGOUT
MENU
Home
Logout
Back

VERIFY DATA DETAILS !!!

Block1 --- is Safe

7. CONCLUSION

In this proposed work, 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 block less 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.

8.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] 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.

[3] 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.

[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 Security, 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 Security, 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, Aug 2017.

[12] 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.

[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,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.