INTERNATIONAL JOURNAL OF
TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

DATA INTEGRITY AUDITING WITHOUT PRIVATE KEY STORAGE FOR SECURE CLOUD STORAGE

VEERAMSETTI SIVA RAMA KRISHNA
PG Scholar, Department of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail: Sivaramveeramsetti@gmail.com

Mr. NAGA. SRINIVASA RAO*
Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail:naagaasrinu@gmail.com

Abstract

Using cloud storage services, users will store their knowledge within the cloud to avoid the expenditure of native knowledge storage and maintenance. to confirm the integrity of the information hold on within the cloud, several knowledge integrity auditing schemes are planned. In most, if not all, of the present schemes, a user must use his non-public key to get the information authenticators for realizing the information integrity auditing. Thus, the user should possess a hardware token (e.g. USB token, sensible card) to store his non-public key and hit the books a arcanum to activate this non-public key. If this hardware token is lost or this arcanum is forgotten, most of this knowledge integrity auditing schemes would be unable to figure. so as to beat this downside, we have a tendency to propose a brand new paradigm known as knowledge integrity auditing while not non-public key storage and style such a theme. during this theme, we have a tendency to use biometric knowledge (e.g. iris scan, fingerprint) because the user's fuzzy non-public key to avoid exploitation the hardware token. Meanwhile, the theme will still effectively complete the information integrity auditing.We utilize a linear sketch with committal to writing and error correction processes to substantiate the identity of the user. additionally, we have a tendency to style a brand new signature theme that not solely supports blockless verifiability, however is also compatible with the linear sketch. the safety proof and therefore the performance analysis show that our planned theme achieves fascinating security and
potency.

Index Terms**: **Biometric, cloud Storage, Private Key, Authentication

I. Introduction

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos, OAuth and OpenID. Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network.

Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server.

One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols. Therefore, in we seek to design a secure and efficient authentication protocol. Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information.

II. LITERATURE SURVEY

Ateniese et al. Firstly proposed the notion of Provable Data Possession (PDP). They employed the random sample technique and homomorphic linear authenticators to design a PDP scheme, which allows an auditor to verify the integrity of cloud data without downloading the whole data from the cloud**.**

Juels and Kaliski proposed the concept of Proof of Retrievability (PoR). In the proposed scheme, the errorcorrecting codes and the spot-checking technique are utilized to ensure the retrievability and the integrity of the data stored in the cloud.

Shacham and Waters constructed two PoR schemes with private verifiability and public verifiability by using pseudorandom function and BLS signature. To support user-interactions, including data modification, insertion and deletion

Zhu et al. Constructed a dynamic data integrity auditing scheme by exploiting the index hash tables.

Sookhak et al. Also considered 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. In public data integrity auditing, the TPA might derive the contents of user's data by challenging the same data blocks multiple times. To protect the data privacy,.

Wang et al. Exploited the random masking technique to construct the first public data integrity auditing scheme supporting privacy preserving.

Li et al. Proposed a data integrity auditing scheme which preserves data privacy from the TPA.

ISSN: 2057-5688

Yu et al. proposed a cloud storage auditing scheme with perfect data privacy preserving by making use of zero-knowledge proof. To relieve the user's computation burden of authenticator generation,

Guan et al. constructed a data integrity auditing scheme using in distinguish ability obfuscation technique, which reduces the overhead for generating data authenticators**.**

Li et al. proposed a data integrity auditing scheme which contains a cloud storage server and a cloud audit server. In this scheme, the cloud audit server helps user to generate data authenticators before uploading data to the cloud storage server. **Shen et al** 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. The data sharing is used widely in cloud storage scenarios. To protect the identity privacy of user,

Wang et al. proposed a shared data integrity auditing scheme based on the ring signature.

Yang et al. designed a remote data integrity auditing scheme for shared data, which supports both the identity privacy and the identity traceability. By using the homomorphic verifiable group signature.

Fu et al. proposed a privacy-aware remote data integrity auditing scheme for shared data. In order to achieve efficient user revocation**.**

Wang et al. designed a shared data integrity auditing scheme supporting user revocation by making use of the proxy re-signature. Based on the identity-based setting.

Zhang et al. constructed a cloud storage auditing scheme for shared data supporting real efficient user revocation. To realize the data sharing with sensitive information hiding.

Shen et al. Designed an identity-based cloud storage auditing scheme for shared data. Other aspects, such as eliminating certificate management and key exposure resilience in data integrity auditing have also been studied. However, all of existing remote data integrity auditing schemes do not take the problem of private key storage into account. In this paper, we explore how to achieve data integrity auditing scheme without private key storage for secure cloud storage.

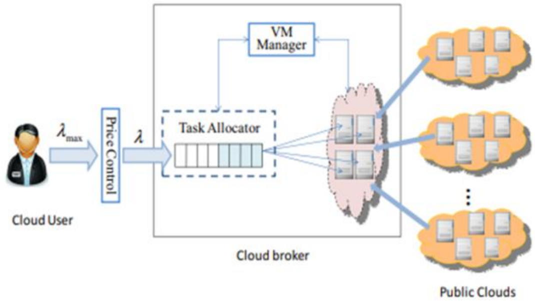
III. PROBLEM STATEMENT

Designed a password based user authentication scheme for wireless sensor networks (WSNs). This is a two-factor authentication scheme as it relies on both a smart card and some password. During the user registration process, an authorized user registers or re-registers with the trusted gateway node (GWN). Althobaiti et al. proposed a biometric-based user authentication mechanism for WSNs. However, their scheme is insecure against impersonation attacks and man-in-the-middle attack. Proposed a new biometric-based user authentication approach.

Disadvantages: In the existing work, the system is less effective due to absence of user finger print image authentication.

The system is less security due to absence of Message Authentication Code.

System Design



IV. MODULES

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.

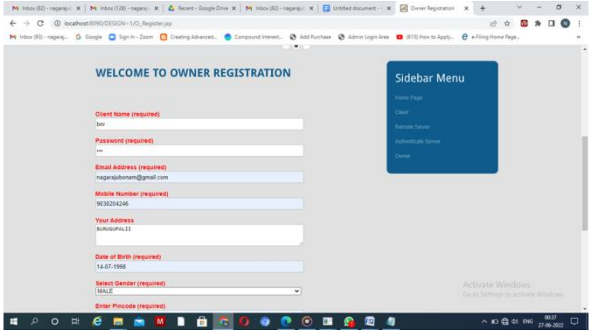
CLOUD SERVER: In this module the cloud will authorize both the owner and the user and also performs the following operations such as View and Authorize Users, View and Authorize Owners,View All File's Blocks,View All Transactions,View All Attackers, View Time Delay Results,View Throughput Results

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

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.

V. RESULTS

Owner registration page


localhost:8090/DESIGN-1/O_Register.jsp

WELCOME TO OWNER REGISTRATION

Client Name (required): bnr

Password (required): •••

Email Address (required): nagarajubonam@gmail.com

Mobile Number (required): 9030204246

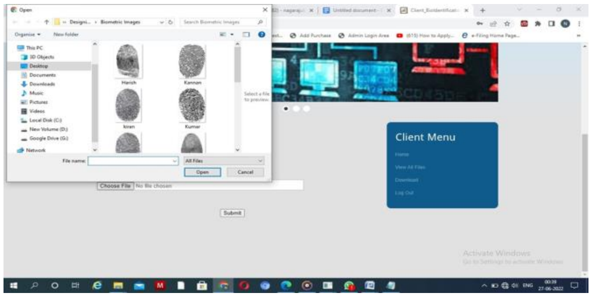
Your Address: BURUGUPALII

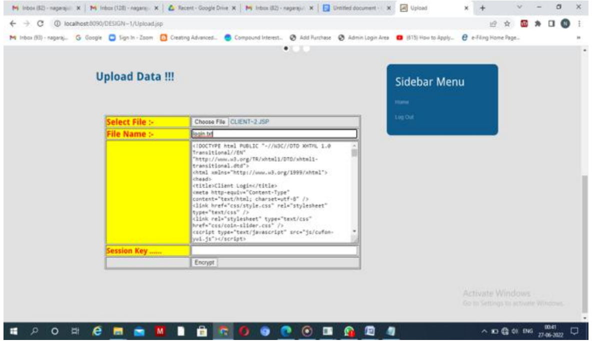
Date of Birth (required): 14-07-1998

Select Gender (required): MALE

Enter Pincode (required)

Biometric choose page





Upload Data !!!

Select File :- CLIENT-2.JSP

File Name :- login.txt

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Client Login</title>
<meta http-equiv="Content-Type"
content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet"
type="text/css" />
<link rel="stylesheet" type="text/css"
href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-
yui.js"></script>
```

Session Key ......

Upload data page

VI. CONCLUSION

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks.

VII. REFERENCES

1. Improving product marketing by predicting early reviewers on E-Commerce websites
S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, “Improving product marketing by predicting early reviewers on E-Commerce websites,” Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. “Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN.” Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40. Accessed 2 May 2024.

3. V. Srikanth, “CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS,” IJTE, pp. 106–109, Jan. 2023, [Online]. Available: http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf

4. V. SRIKANTH, “DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS,” International Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf

5. V. SRIKANTH, “A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES,” IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023,

[Online]. Available: http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Detection of fake currency using machine learning models," Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. "Cyberspace and the Law: Cyber Security." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. "Data Structures Laboratory Manual." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

9. Data Analytics Using R Programming Lab." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)," journal-article, 2019. [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf

10. V. SRIKANTH, "Secured ranked keyword search over encrypted data on cloud," IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION," IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS," Feb. 2017. [Online]. Available: http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

14 Srikanth, V. 2018. "Secret Sharing Algorithm Implementation on Single to Multi Cloud." International Journal of Research 5 (01): 1036–41. https://journals.pen2print.org/index.php/ijr/article/view/11641/11021.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. “Intelligents Traffic Light Controller for Ambulance.” Journal of Image Processing and Intelligent Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, https://doi.org/10.55529/jipirs.34.19.26. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. “Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges.” Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023, pp. 1–7, https://doi.org/10.55529/jeet.35.1.7. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023