ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/04.2024-74345916/IJAEAST.2024.02.0001, February 2024, Volume-2, Issue-2, pp.49-56
International Journal of Advances in Engineering Architecture Science and Technology

Secure and Efficient Online Fingerprint Authentication Scheme Based on Cloud Computing

M. Amareswara Kumar[1], T. Mahesh[2], V. Reddy Ganesh[3], G. Venkata Sai[4], O. Diwakar[5]

[1]Assisttant Professor, Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal, Andhra Pradesh, India

[2,3,4,5]Student, Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal, Andhra Pradesh, India

amar.cse@srecnandyal.edu.in[1], 20x51a05b5@srecnandyal.edu.in[2], 20x51a05b9@srecnandyal.edu.in[3], 21x55a0503@srecnandyal.edu.in[4], 20x51a0598@srecnandyal.edu.in[5]

Received: 23-01-2024 **Accepted:** 19-02-2024 **Published:** 24-02-2024

Abstract

Background: The e-Finga online fingerprint authentication system, while efficient, is vulnerable to privacy breaches due to its use of deterministic encryption.
Objectives: Researchers found that adversaries could potentially exploit this to steal fingerprint data. To enhance security, the Secure e-finger scheme was introduced, employing a more complex encryption method that still allows for quick computations and minimal communication overhead.
Statistical Analysis: This upgrade increases the client's running time slightly by 6% but offers a substantial improvement in privacy protection, effectively blocking the identified attack without sacrificing performance. Additionally, a threshold scheme is suggested to prevent excessive access rights for single users. The e-Finga scheme for fingerprint authentication is at risk of privacy leaks due to its predictable encryption method. Attackers can exploit this to access user's fingerprint data.
Findings: To fix this, the Secure e-finger scheme applies a more secure encryption, slightly increasing running time but greatly enhancing user privacy without significantly impacting efficiency. A threshold scheme is also proposed to limit user access rights.
Applications and Improvements: The topic is chosen due to the critical need for robust privacy protection in biometric authentication systems. As biometrics are unique and immutable, a breach can have severe and permanent implications for an individual's privacy and security, making the development of more secure systems like Secure e-finger both timely and essential.

Keywords: e-Finga, Fingerprint Authentication, Cloud Computing, Authentication, Security.

1. Introduction

Increasingly use of mobile and the evolution of biometric technology has sparked widespread interest in bi identification for individual authentication. Biometric, based on personal or behavioral characteristics, a promising avenue for authentication. However, growing sensitivity

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/04.2024-74345916/IJAEAST.2024.02.0001, February 2024, Volume-2, Issue-2, pp.49-56
International Journal of Advances in Engineering Architecture Science and Technology

of bi data has raised significant concerns. Addressing challenge, our motivation to develop a novel- preserving online fingerprint scheme, named e-Finga, designed operate over encrypted outs data. The primary objective the project is to and implement e-Fa, a privacy securing online fingerprint authentication. The goal is to users to outsource fingerprint data to authorized, ensuring secure, and efficient authentication without compromising the confidentiality of the fingerprint information. The project aims to employ improve homomorphic encryption technology for secure Euclidean distance calculation, facilitating an efficient online fingerprint algorithm over encrypted FingerCode data in outsourcing scenarios. The objective of this projects is to address privacy concerns associated with biometric data in the context of online fingerprint authentication. The proposed solution, e-Finga, introduces a novel privacy-preserving scheme leveraging homomorphic encryption. It allows users to securely outsource their fingerprint data to authorized servers, ensuring accurate and efficient authentication without compromising sensitive information. The improved homomorphic encryption technology enables secure Euclidean distance calculations, facilitating online fingerprint matching over encrypted FingerCode data. The project aims to provide a robust defence against various security threats, as validated through detailed security analyses. Implementation on a real fingerprint database demonstrates e-Finga's efficiency and accuracy in online fingerprint authentication.". The scope of the extend envelops the advancement and arrangement of e-Finga, amplifying to real-world applications of online unique mark confirmation. The centre lies on accomplishing a vigorous framework able of standing up to different security dangers whereas giving consistent and exact confirmation administrations. The scheme's scope incorporates usage over a workstation with a veritable unique finger impression database, and its productivity and precision will be approved through broad reenactment comes about. In later a long time, the expanding ubiquity of portable gadgets and the progressions in biometric innovation have moved the intrigued in biometric recognizable proof for person confirmation. Leveraging individual organic or behavioural characteristics, biometric verification has gotten to be an fundamentally portion of security frameworks. In any case, the delicate nature of biometric information has raised critical security concerns. This paper addresses these challenges and presents a groundbreaking privacy-preserving online unique mark verification plot called e-Finga, outlined to function over scrambled outsourced information.

2. Literature Survey

The referenced paper explores the domain of online fingerprint authentication, with a specific focus on efficiency and privacy preservation through the use of encrypted outsourced data. By leveraging the 2017 IEEE International Conference on Communications as a platform, the authors delve into the intricacies of achieving a balance between computational efficiency and robust privacy measures in the context of fingerprint-based authentication.

The motivation behind this project is rooted in the increasing reliance on biometric data for user authentication and the corresponding privacy concerns associated with such sensitive information. The authors aim to address these challenges by proposing an innovative approach that not only ensures the efficiency of online fingerprint authentication but also preserves the privacy of the user's biometric data through encryption when outsourced to different servers. The project introduces a novel scheme named e-Finga, designed to achieve privacy-preserving online fingerprint authentication over encrypted outsourced data. The authors present an improved homomorphic encryption technology tailored for secure Euclidean distance calculation, forming the basis of an efficient online fingerprint matching algorithm. The key contribution lies in enabling the outsourcing of a user's fingerprint, registered with a trusted

authority, to multiple servers with user authorization, ensuring a secure and accurate authentication process without compromising the confidentiality of the fingerprint information. This reference will make the data of the users in the cipher text and data will be unable to understand for the hackers. Data will be given in the form of cipher model and given data will be managed by the trusted authority. The trusted authority will take over all the properties of the data and manage the data. This reference explores the realm of gait authentication on mobile phones, employing a combination of biometric cryptosystems and fuzzy commitment schemes. The authors delve into the nuances of securing mobile devices through gait-based authentication, contributing to the broader field of information security. The motivation behind this project stems from the need for robust authentication mechanisms on mobile phones, considering the ubiquity and vulnerability of these devices. By utilizing gait as a unique biometric identifier and incorporating cryptographic techniques, the authors aim to enhance the security of mobile devices against unauthorized access.

The project introduces a gait authentication system for mobile phones, integrating a biometric cryptosystem and a fuzzy commitment scheme. The objective is to establish a secure and reliable authentication method that harnesses the distinctive characteristics of an individual's gait. Through the International Journal of Information Security, the authors present findings that contribute to the ongoing efforts to fortify the security posture of mobile devices in an increasingly interconnected world. This reference investigates a comparative competitive coding approach for personal identification by fusing finger vein and finger dorsal texture information. The study explores the use of dual biometric features to enhance the accuracy and reliability of personal identification systems. The motivation behind this project lies in the pursuit of improving personal identification systems through the fusion of multiple biometric traits. The authors aim to demonstrate the effectiveness of combining finger vein and finger dorsal texture information in a comparative competitive coding framework to achieve superior accuracy in personal identification. The project introduces a novel approach to personal identification through the fusion of finger vein and finger dorsal texture information. By leveraging a comparative competitive coding framework, the authors aim to enhance the accuracy and reliability of identification systems. The project, published in Information Sciences, contributes valuable insights into the development of more robust and secure personal identification methods. This reference explores the evolving landscape of biometric authentication, specifically focusing on the potential replacement of traditional bank passwords with fingerprint-based authentication. The motivation behind this exploration is rooted in the increasing need for secure and user-friendly authentication methods in the financial sector. The article underscores the growing trend of integrating fingerprint readers as a means of enhancing security and user convenience in banking applications. The article introduces the idea that fingerprints are on the verge of replacing traditional bank passwords. Highlighting the trend, the author discusses the implications of incorporating fingerprint readers in banking technology, emphasizing the potential benefits in terms of security and user experience. This forward-looking perspective sheds light on the transformative impact of biometric authentication in the financial sector. This reference reports on HSBC's implementation of a voice and fingerprint ID system for its customers, exploring the integration of biometric authentication into the banking sector. The motivation behind this report is driven by the financial industry's pursuit of advanced security measures and the adoption of cutting-edge biometric technologies. HSBC's initiative to offer voice and fingerprint ID aims to enhance customer security and streamline authentication processes.

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/04.2024-74345916/IJAEAST.2024.02.0001, February 2024, Volume-2, Issue-2, pp.49-56
International Journal of Advances in Engineering Architecture Science and Technology

3. System Analysis and Design

Existing System

Within the current scene, versatile gadgets broadly utilize biometric innovation for person verification. Be that as it may, the winning protection concerns related with biometric information, owing to its profoundly delicate nature, posture noteworthy challenges. Existing frameworks frequently need strong components to address these protection issues. Biometric information, particularly fingerprints, may be put away without satisfactory security, driving to potential security breaches and unauthorized get to. The nonappearance of proficient privacy-preserving measures compromises client privacy.

Disadvantages

Need of satisfactory protection measures may uncover biometric information to unauthorize id entities. Existing frameworks may not adequately stand up to different security dangers, putting touchy data at hazard.

Proposed System

In response to the impediments of the existing framework, the proposed e-Finga plot offers a pioneering privacy-preserving online unique fingerprint verification solution over encrypted outsourced data. This novel approach ensures that a user's fingerprint, registered with a trust agent, can be securely outsourced to various servers with user permission. The proposed framework incorporates an advanced homomorphic encryption technology for secure Euclidean distance calculation, enhancing the efficiency of the online fingerprint matching algorithm in outsourcing scenarios.

Advantages

e-Finga ensures privacy conservation, shielding against unauthorized access and data leakage. Fingerprint data can be outsourced securely to different servers, preventing compromise of sensitive data.

4. System Architecture

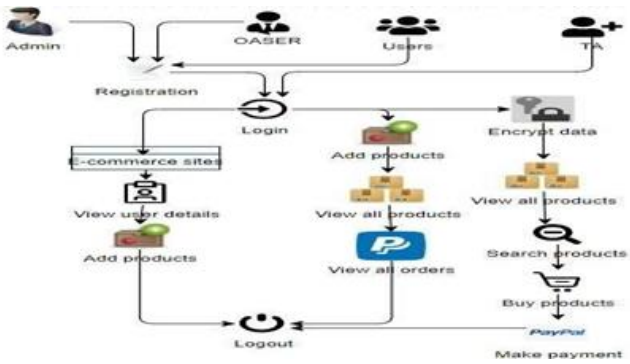


Figure 1. Architecture for Authentication Scheme

5. Modules

Admin Module

Login: The administrator can login with using default valid credentials.
E-Commerce Sites: The admin can view the added e-commerce sites URLs along with logo.

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/04.2024-74345916/IJAEAST.2024.02.0001, February 2024, Volume-2, Issue-2, pp.49-56
International Journal of Advances in Engineering Architecture Science and Technology

User details: The admin can view the registered users.
Add Products: The admin can add the products brands and categories
Logout: The admin should be logout.

User Module

Create account: The user needs to create their account providing like name, mobile, pin, fingerprint.
Login: The user can login with using valid credentials.
Encrypt user details: The user will encrypt the user details for security purpose.
View all products: The user can view the all products.
Search products: The user has an option to search products by product brand and category type.
Buy Now: The user needs to add user details for buy the products like address, payment mode, and count etc.,
Make payment: If the user wants to process the product, he needs to add the payment method.
My orders: The user can view the ordered products.
Logout: The user should be logout.

OASERS Module

Register: The OASER will register with providing their product, prize, logo, URL, etc.
Login: The OASER can login with using their valid credentials.
Add products: The OASER has a access to add the products
View all products: he can view the all added products.
View user orders: The owner can view the ordered users.
Logout: Owner should be logout.

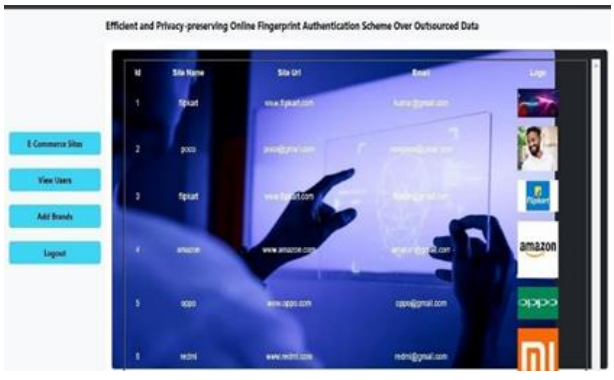
TPA module

Login: TAs has a default credentials, he can login with directly using default credentials.
Sent request to OAS: The TA need to send a user order request to OAS.
Logout: The TA should be logout

6. Result And Discussion

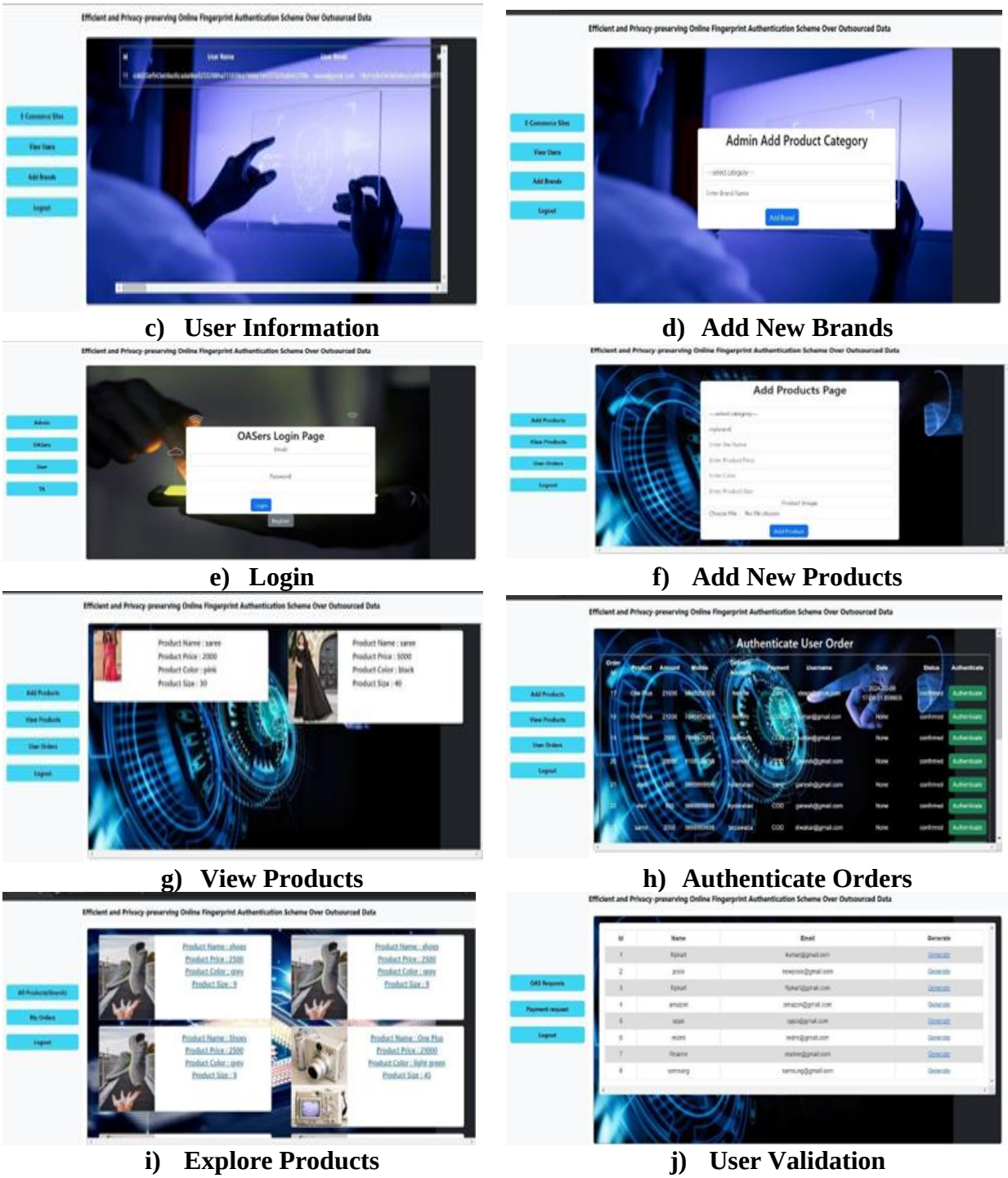
Secure and Efficient Online Fingerprint Authentication Scheme Using Cloud Computing. In this project to know the original user is using the site or any others are using the site will be known and can be prevent the fake orders in the user's E-Commerce account.

a) Admin Page



b) E-Commerce Sites

ISSN: 2583-7346
DOI: https://doi-ds.org/doilink/04.2024-74345916/IJAEAST.2024.02.0001, February 2024, Volume-2, Issue-2, pp.49-56
International Journal of Advances in Engineering Architecture Science and Technology



c) User Information
d) Add New Brands
e) Login
f) Add New Products
g) View Products
h) Authenticate Orders
i) Explore Products
j) User Validation

Figure 1. Developed Modules

7. Conclusion

The e-Finga scheme represents a significant step forward in addressing privacy concerns related to biometric data in online fingerprint authentication. Through the utilization of advanced homomorphic encryption technology, the scheme securely transfers users' fingerprints to authorized servers, allowing for efficient and accurate authentication while safeguarding sensitive information. The introduction of secure Euclidean distance calculations enhances the

online fingerprint matching algorithm, bolstering the system's overall robustness. Extensive security analyses confirm the scheme's resilience against various threats, instilling confidence in its practical application. The fingerprint authentication system is used in a variety of applications, such as access control, identity management, and other forms of authentication. It is also used in law enforcement and government agencies, as it provides a reliable and cost-effective way to identify and authenticate individuals. Each fingerprint examination will result in one of the following conclusions: The fingerprint was made by (identified/individualized to) a known source (victim, suspect, etc.) The fingerprint was not made by (excluded to) a known source. The fingerprint cannot be identified or excluded to a known source (inconclusive). The biometric system may find applications in attendance system, security systems, and identification purposes and may find even more applications in the time to come. The prevalent systems would be worked upon and modified for error free secure system. Fingerprint recognition technology offers numerous advantages for smart door locks, including enhanced security, convenience, flexibility, easy installation, and compatibility with other smart home devices and systems.

References

1. Mahammad, F. S., & Viswanatham, V. M. (2020). Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach. The Journal of Supercomputing, 76(4), 2275-2288.
2. Karukula, N. R., & Farooq, S. M. (2013). A route map for detecting Sybil attacks in urban vehicular networks. Journal of Information, Knowledge, and Research in Computer Engineering, 2(2), 540-544.
3. Farook, S. M., & NageswaraReddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. Inter national journal of Scientific Engineering and Technology Research, 4(0), 41.
4. Sunar, M. F., & Viswanatham, V. M. (2018). A fast approach to encrypt and decrypt of video streams for secure channel transmission. World Review of Science, Technology and Sustainable Development, 14(1), 11-28.
5. Mahammad, F. S., & Viswanatham, V. M. (2017). A study on h. 26x family of video streaming compression techniques. International Journal of Pure and Applied Mathematics, 117(10), 63-66.
6. Devi,S M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M., & Swathi, P. V. (2022).” Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection.” Journal of Algebraic Statistics, 13(3), 112-117.
7. Devi, M. M. S., & Gangadhar, M. Y. (2012).” A comparative Study of Classification Algorithm for Printed Telugu Character Recognition.” International Journal of Electronics Communication and Computer Engineering, 3(3), 633-641.
8. Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M. MISSING CHILD IDENTIFICATION SYSTEM USING DEEP LEARNING.
9. V. Lakshmi chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13, no. 2 (2022): 2477-2483.

10. Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori vs Genetic algorithms for Identifying Frequent Item Sets. International journal of Innovative Research &Development, 3(6), 249-254.
11. Chaitanya, V. L., Sutraye, N., Praveeena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental Investigation of Machine Learning Techniques for Predicting Software Quality.
12. Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware with an Enhanced Genetic Algorithm for Feature Selection and Machine Learning.
13. Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity checking in Public Cloud. International Journal of Research, 5(22), 744-757.
14. Lakshmi, B. S. (2021). Fire detection using Image processing. Asian Journal of Computer Science and Technology, 10(2), 14-19.
15. Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C. Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language.
16. Kumar, M. A., Mahammad, F. S., Dhanush, M. N., Rahul, D. P., Sreedhara, K. L., Rabi, B. A., & Reddy, A. K. (2022). Traffic Length Data Based Signal Timing Calculation for Road Traffic Signals Employing Proportionality Machine Learning. Journal of Algebraic Statistics, 13(3), 25-32.
17. Kumar, M. A., Pullama, K. B., & Reddy, B. S. V. M. (2013). Energy Efficient Routing In Wireless Sensor Networks. International Journal of Emerging Technology and Advanced Engineering, 9(9), 172-176.
18. Kumar, M. M. A., Sivaraman, G., Charan Sai, P., Dinesh, T., Vivekananda, S. S., Rakesh, G., & Peer, S. D. BUILDING SEARCH ENGINE USING MACHINE LEARNING TECHNIQUES.