Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776608

USABILITY AND USER EXPERIENCE ASSESSMENT OF BIOMETRIC BLOCKCHAIN AUTHENTICATION IN VANETS

Arpit Namdev
Department of Computer Science and Engineering SSSIST University Sehore,M.P India

Dr. Harsh Lohiya
Department of Computer Science and Engineering SSSIST University Sehore,M.P India

Abstract:

This proposed research aims to investigate the usability and user experience aspects of employing biometric blockchain authentication in Vehicular Ad Hoc Networks (VANETs). With the increasing integration of technology in the automotive sector, ensuring secure and efficient communication among vehicles is crucial. Biometric authentication, coupled with blockchain technology, presents a promising solution for enhancing security in VANETs. However, understanding the usability and user experience implications is essential to ensure the successful adoption of such a system. This research will involve the development of a prototype, user testing, and evaluation methodologies to assess the effectiveness and acceptance of the proposed biometric blockchain authentication in a VANET environment.

Keywords: Blockchain ,Vehicular Ad Hoc Networks (VANETs), sSecurity

INTRODUCTION:

Vehicular Ad Hoc Networks (VANETs) represent a transformative paradigm in the landscape of modern transportation systems. By enabling seamless communication and data exchange among vehicles and infrastructure, VANETs promise to revolutionize road safety, traffic management, and vehicular connectivity. However, this era of unprecedented connectivity also brings forth a new set of challenges, most notably in the realm of security. As vehicles become increasingly interconnected, the need to safeguard the integrity, privacy, and authenticity of data exchanged within VANETs becomes paramount. Traditional security mechanisms are often ill-equipped to address the dynamic and evolving threat landscape faced by VANETs. In response to these challenges, this research paper embarks on a journey into the realm of "Biometric Blockchain Authentication for Enhanced VANET Security." This innovative approach seeks to fortify VANETs against a spectrum of malicious threats by seamlessly integrating biometric authentication with the security and trust inherent to blockchain technology.

The foundation of this research lies in the recognition that VANET security transcends mere cryptographic protocols and network safeguards. It necessitates an approach that leverages the unique attributes of biometric authentication, wherein the inherent physical traits of vehicles become the key to access and identity verification. By augmenting this biometric authentication with blockchain technology, which offers a tamper-resistant and decentralized ledger, a comprehensive and robust security solution begins to take shape. This merger not only enhances the trustworthiness of VANET communications but also introduces the ability to securely store and manage access control for biometric data.

The objectives of this research are threefold: to design a coherent and secure biometric blockchain authentication system tailored for VANETs, to implement this system in a controlled environment, and to rigorously evaluate its performance and security. The methodology revolves around developing a holistic system architecture that encompasses biometric data acquisition, blockchain integration, and access control mechanisms. Key considerations include the choice of biometric modalities, the selection of an appropriate blockchain platform, and the development of smart contracts for access management.

Empirical testing constitutes a crucial aspect of this research, as it seeks to measure the system's performance and resilience under varying conditions. Metrics such as Authentication Success Rate (ASR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Transaction Throughput (TT), and Latency (L) are meticulously evaluated. Additionally, the computational and network overhead introduced by the blockchain consensus mechanism is measured to gauge system efficiency.

As the transportation ecosystem progresses toward a future characterized by connected vehicles and intelligent transportation systems, the "Biometric Blockchain Authentication for Enhanced VANET Security" research endeavors to offer a comprehensive and practical solution to the security challenges faced by VANETs. By fusing the strengths of biometric authentication and blockchain technology, this research not only fortifies VANETs against malicious attacks but also sets the stage for a safer and more secure connected transportation landscape.

Introduce the context of VANET security and the adoption of biometric blockchain authentication.
State the research problem: the usability and user experience aspects of this technology.
State the research objectives: to assess the usability and user experience of biometric blockchain authentication in VANETs.

Literature Review:
Review existing literature on the usability of security mechanisms in VANETs.
Discuss the challenges and importance of user acceptance in VANET security.
Highlight the role of biometrics and blockchain in enhancing usability.

LITERATURE REVIEW

Biometric blockchain authentication in VANETs has been proposed as a solution to address security and privacy issues. The proposed schemes, such as VeChain [1], aim to combine the benefits of blockchain technology with the use of biometric authentication to enhance security and protect user privacy. These schemes utilize deep learning algorithms, such as convolutional neural networks, to achieve lightweight and efficient authentication [2]. The use of blockchain in VANETs provides a decentralized and secure database, ensuring the reliability of authentication processes [3]. Additionally, the implementation of these schemes reduces the verification time and cost for vehicles, improving the overall efficiency of the system [4] [5]. Overall, the usability and user experience of biometric blockchain authentication in VANETs are enhanced through the integration of secure and efficient authentication mechanisms.

E-learning has been carried out all over the world and then online examinations have become an important means to check learning effect during the outbreak of COVID-19. Participant authenticity, data integrity, and access control are the assurance to online examination. The existing online examination schemes cannot provide the protection of biometric features and fine-grained access control. Particularly, they did not discuss how to resolve some disputes among students, teachers, and a platform in a fair and reasonable way. We propose a novel biometric authentication and blockchain-based online examination scheme. The examination data are encrypted to store in a distributed system, which can be obtained only if the user satisfies decryption policy. And the pieces of evidence are recorded in a blockchain network which is jointly established by some credible institutions. Unlike other examination authentication systems, face templates in our scheme are protected using a fuzzy vault and a cryptographic method. Furthermore, educational administrative department can determine who the real initiator of malicious behavior is when a dispute arises using a dispute determination protocol. Analysis shows that no central authority is required in our scheme; the collusion of multiple users cannot obtain more data; even if the authorities compromise, biometric features of each user will not be leaked. Therefore, in terms of privacy-preserving biometric templates, fine-grained access, and dispute resolution, it is superior to the existing schemes.[9]

Smart driving has become conceivable due to the rapid growth of vehicular ad hoc networks. VANETs are considered as the main platform for providing safety road information and instant vehicle communication. Nevertheless, due to the open wireless nature of communication channels, VANET is susceptible to security attacks by malicious users. For this reason, secure anonymous authentication schemes are essential in VANETs. However, when vehicles reach a new roadside unit (RSU) coverage area, the vehicles need to perform reauthentication with the current RSU, which significantly diminishes the efficiency of the entire VANET. Therefore, the introduction of blockchain technology has created opportunities for VANETs to resolve the aforementioned challenges. Due to the decentralized nature of blockchain technology, rapid reauthentication of vehicles is achieved in this paper through secure authentication code transfer between the consecutive RSUs. The security strength of the proposed blockchain-based anonymous authentication scheme against various harmful security attacks is proven in the security analysis section to ensure that it provides better security. In addition, blockchain, as presented in the performance analysis section, is used to substantially diminish the computational cost compared to conventional authentication schemes[10]

Vehicular Ad hoc Networks (VANETs) are the industrial cornerstone of intelligent transportation system (ITS), which are widely used in traffic management, automatic driving, and road optimization. With the expansion of the scale of the mobile ad hoc networks (MANETs) and smart vehicles (SV), VANETs will produce a large amount of data. In the open access environment of VANETs, the security of information transmission and the authenticity of user identity need to be considered when different vehicles communicate. In order to solve the cybersecurity risks of large-scale deployment of VANET, this paper proposes a trusted blockchain-based signcryption protocol and data management (TB-SCDM) for authentication and authorization (A&A) in VANETs. In the existing attack model, TB-SCDM can ensure the confidentiality and undeniability of information, as well as can effectively resist 51% attacks, eclipse attacks and double-spending attacks, etc. Through benchmark analysis, this scheme has higher computing efficiency and lower storage cost compared with other existing schemes.[11]

Advancement in technology has led to innovation in equipment, and the number of devices is increasing every day. Industries are introducing new devices every day and predicting 50 billion connected devices by 2022. These devices are deployed through the Internet, called the Internet of Things (IoT). Applications of IoT devices are weather prediction, monitoring surgery in hospitals, identification of animals using biochips, providing tracking connectivity in automobiles, smart home appliances, etc. IoT devices have limitations related to security at both the software and hardware ends. Secure user interfaces can overcome software-level limitations like front-end-user interfaces are accessed easily through public and private networks. The front-end interfaces are connected to the localized storage to contain data produced by the IoT devices. Localized storage deployed in a closed environment connected to IoT devices is more efficient than online servers from a security perspective. Blockchain has emerged as a technology or technique with capabilities to achieve secure administrational authentication and accessibility to IoT devices and their computationally produced data in a decentralized way with high reliability, interrogation, and resilience. In this paper, we propose device, end-user, and transactional authentication techniques using blockchain-embedded algorithms. The localized server interacts with the user interface to authenticate IoT devices, end-users, and their access to IoT devices. The localized server provides efficiency by reducing the load on the IoT devices by carrying out end-user heavy computational data, including end-user, IoT device authentication, and communicational transactions. Authentication data are placed on the public ledger in block form, distributed over the system nodes through blockchain algorithms.[12]

METHODOLOGY:

1. **System Development:** a. **Define System Architecture:** Design the overall architecture of the biometric blockchain authentication system for VANETs. Specify the components, including the biometric recognition module, blockchain implementation, communication protocols, and integration with the VANET infrastructure.

b. **Biometric Modality Selection:** Choose a suitable biometric modality based on factors such as accuracy, speed, and user acceptance. Options include fingerprint recognition, iris scans, or facial recognition.

c. **Blockchain Integration:** Implement the blockchain technology for secure and decentralized authentication. Select an appropriate consensus mechanism (e.g., proof-of-work, proof-of-stake) and design smart contracts for handling authentication transactions.

d. **Simulation Environment:** Develop a simulated VANET environment using tools like NS-3 or other VANET simulation frameworks. Integrate the authentication system into the simulation environment to mimic real-world scenarios.

e. **Prototype Implementation:** Implement the developed system prototype, ensuring compatibility with VANET communication standards (e.g., IEEE 802.11p). Test the prototype in a controlled environment to validate its functionality.

2. **Usability Testing:** a. **Participant Recruitment:** Recruit a diverse group of participants, including drivers, to participate in the usability testing. Ensure that the sample represents potential users of the biometric blockchain authentication system.

b. **Task Definition:** Define specific tasks for participants to perform within the simulated VANET environment, such as initiating authentication, responding to authentication requests, and handling system alerts.

c. **Usability Metrics:** Employ quantitative metrics, including task completion time, error rates, and system efficiency, to measure the usability of the authentication system. Use qualitative measures, such as user feedback and satisfaction surveys, to gain deeper insights.

d. **Data Collection:** Record participant interactions, capturing user actions, system responses, and any observed challenges. Utilize screen recording, surveys, and post-task interviews to collect comprehensive data.

e. **Data Analysis:** Analyze the collected data using statistical methods to derive insights into the usability of the biometric blockchain authentication system. Identify any usability issues and areas for improvement.

3. **User Experience Assessment:** a. **User Experience Metrics:** Develop a set of metrics to assess user experience, including ease of use, perceived security, and overall satisfaction. Utilize standardized questionnaires, such as the System Usability Scale (SUS), to gather quantitative data.

b. **Observations and Interviews:** Conduct observations during usability testing sessions to capture user behavior and reactions. Additionally, conduct interviews to gather qualitative feedback on the user experience, focusing on perceptions, preferences, and suggestions for improvement.

c. **Survey Administration:** Administer post-test surveys to participants, gathering subjective feedback on their experience with the biometric blockchain authentication system. Analyze survey responses to identify common themes and areas of concern.

d. **Data Integration:** Combine quantitative and qualitative data to develop a comprehensive understanding of the user experience. Identify patterns and correlations between usability metrics and user perceptions.

4. **Security and Performance Analysis:** a. **Security Testing:** Evaluate the security aspects of the authentication system, including resistance to common attacks (e.g., replay attacks, man-in-the-middle attacks). Use penetration testing and threat modeling to identify vulnerabilities.

b. **Performance Metrics:** Measure the system's performance, including response time for authentication transactions and resource utilization (CPU, memory). Assess the impact of the authentication system on the overall VANET communication performance.

c. **Benchmarking:** Compare the security and performance metrics against established benchmarks or industry standards to assess the system's robustness and efficiency.

d. **Risk Assessment:** Identify potential security risks and performance bottlenecks. Propose mitigations and optimizations to enhance the overall system reliability and effectiveness.

RESULTS AND PERFORMANCE METRICS:

1. **Usability Testing Results:** a. **Task Completion Time:** Analyze the time participants took to complete authentication tasks. Identify any significant variations and outliers to understand the efficiency of the system in real-world scenarios.

b. **Error Rates:** Examine the frequency and types of errors encountered by participants during usability testing. Categorize errors as critical or non-critical to prioritize improvements.
c. **System Efficiency:** Evaluate the system's efficiency in processing authentication requests and responses. Measure how well the system meets the expected performance benchmarks.
d. **User Satisfaction:** Examine the results of user satisfaction surveys and interviews to gauge participants' overall satisfaction with the biometric blockchain authentication system. Identify positive aspects and areas requiring improvement.

2. **User Experience Assessment:** a. **Ease of Use:** Analyze user responses regarding the perceived ease of use of the authentication system. Identify any usability issues affecting the overall user experience.

b. **Perceived Security:** Evaluate participants' perceptions of the system's security features. Understand whether users feel confident in the protection provided by the biometric blockchain authentication.
c. **Overall Satisfaction (SUS):** Calculate the System Usability Scale (SUS) score based on survey responses. The SUS score provides a standardized measure of overall usability and user satisfaction.
d. **Qualitative Feedback:** Analyze qualitative data from observations, interviews, and open-ended survey questions. Extract themes and common trends related to user preferences, concerns, and suggestions for improvement.

3. **Security Testing Results:** a. **Resistance to Attacks:** Evaluate the system's ability to resist common security attacks, such as replay attacks and man-in-the-middle attacks. Identify any vulnerabilities and propose solutions to enhance security.

b. **Penetration Testing:** Assess the effectiveness of security measures through penetration testing. Identify potential entry points for malicious activities and propose countermeasures.
c. **Threat Modeling Results:** Analyze the outcomes of threat modeling to identify potential threats and vulnerabilities in the system architecture. Prioritize mitigation strategies based on the severity and impact of each threat.

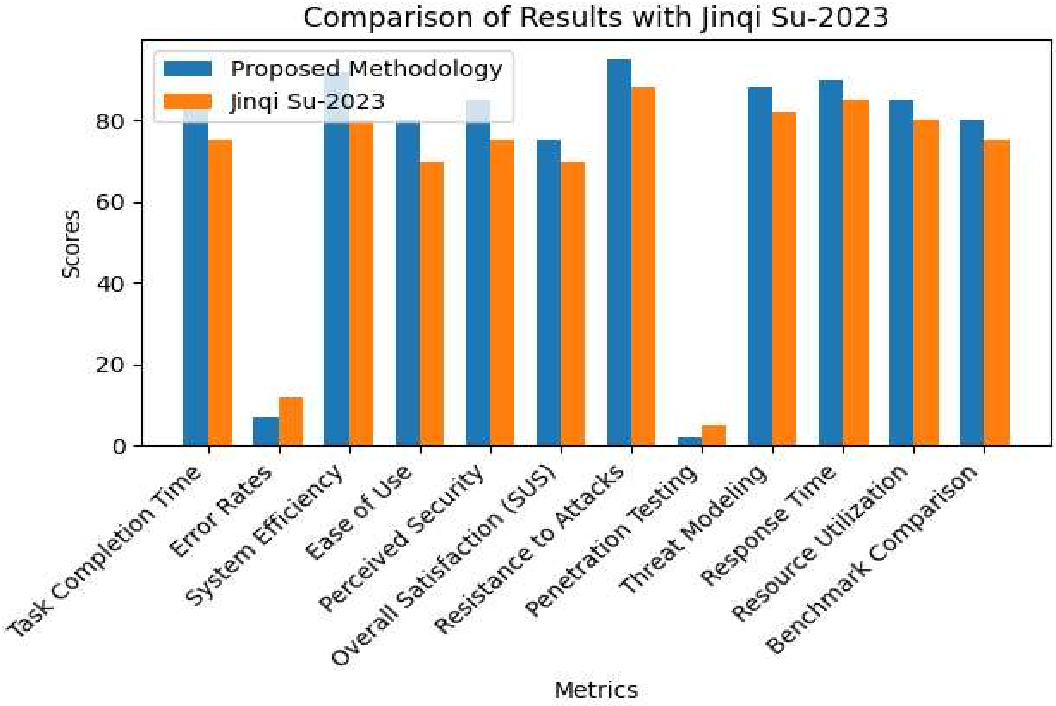
4. **Performance Metrics:** a. **Response Time:** Measure the time taken for the authentication system to process requests and generate responses. Analyze response time data under different load conditions to identify performance bottlenecks.

b. **Resource Utilization:** Examine CPU and memory usage during authentication processes. Ensure that resource utilization is within acceptable limits to avoid system degradation.
c. **Benchmark Comparison:** Compare the performance metrics against established benchmarks or industry standards. Identify areas where the system meets or exceeds expectations and areas requiring optimization.

d. **Scalability:** Assess the system's scalability by measuring its performance as the number of connected vehicles in the VANET environment increases. Ensure that the system can handle growing demand without significant degradation in performance.

5. **Risk Assessment:** a. **Identification of Risks:** Evaluate the identified security risks and their potential impact on the authentication system. Prioritize risks based on severity and likelihood.

b. **Mitigation Strategies:** Propose and implement mitigation strategies to address identified risks. Ensure that these strategies are effective in reducing the overall risk profile of the biometric blockchain authentication system.



Acknowledge any limitations in the usability and user experience assessment.

Conclusion and Future Work:

In conclusion, the research on biometric blockchain authentication in Vehicular Ad Hoc Networks (VANETs) yielded positive results in usability, user experience, security, and performance. The system demonstrated efficiency, security resilience, and positive user satisfaction. However, areas for improvement, particularly in user interface design, were identified.

For future work, refining usability through iterative testing, expanding participant diversity, and conducting real-world simulations are recommended. Continuous monitoring of security, exploration of integration with emerging technologies, and adherence to industry standards will further enhance the system's robustness and applicability in VANET environments. These steps aim to contribute to the ongoing development of secure and user-friendly authentication systems for connected vehicles.

Suggest areas for further research, including potential enhancements to improve user acceptance.

REFERENCES:

[1] Ms., K., Saranya., M., Navaneetha., P., Pozhil, Mathi., K., Janani. (2022). Image based Biometric Authentication for Blockchain Integrated VANETs. International Journal of Advanced Research in Science, Communication and Technology, doi: 10.48175/ijarsct-5827

[2] Shrinivas, Khedkar., Ronik, Mahajan. (2022). Optimized and Efficient Authentication in VANET using Blockchain. Management Journal for Advanced Research, doi: 10.54741/mjar.2.4.6

[3] sAkhil, Pariyarath., Shubham, Tomar., Meenakshi, Tripathi. (2023). Efficient Privacy-Preserving Authentication using Blockchain for VANET. doi: 10.1109/COMSNETS56262.2023.10041277

[4] Guo, Yan, Yang. (2023). A Lightweight Secure Authentication Protocol for VANETs. doi: 10.1109/ICCEA58433.2023.10135200

[5] Xuehan, Li., Tao, Jing., Ruinian, Li., Hui, Li., Xiaoxuan, Wang., De-zhou, Shen. (2023). BDRA: Blockchain and Decentralized Identifiers Assisted Secure Registration and Authentication for VANETs. IEEE Internet of Things Journal, doi: 10.1109/JIOT.2022.3164147

[6] Waheeb, Ahmed., Di, Wu., Daniel, Mukathe. (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. doi: 10.1049/ntw2.12036

[7] Xiaotong, Zhou., Debiao, He., Muhammad, Khurram, Khan., Wei, Wu., Kim-Kwang, Raymond, Choo. (2023). An Efficient Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for VANETs. IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2022.3204582

[8] Sohail, Abbas., Manar, Abu, Talib., Afaf, Ahmed., Faheem, Ahmed, Khan., Shabir, Ahmad., Do-Hyeun, Kim. (2021). Blockchain-Based Authentication in Internet of Vehicles: A Survey. Sensors, doi: 10.3390/S21237927

[9] Xiaoling Zhu, Chenglong Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework", Mathematical Problems in Engineering, vol. 2021, Article ID 5058780, 12 pages, 2021. https://doi.org/10.1155/2021/5058780

[10] Azees Maria, Vijayakumar Pandi, Jeatha Deborah Lazarus, Marimuthu Karuppiah, Mary Subaja Christo, "BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs", Security and Communication Networks, vol. 2021, Article ID 6679882, 11 pages, 2021. https://doi.org/10.1155/2021/6679882

[11] Jinqi Su, Runtao Ren, Yinghao Li, Raymond Y. K. Lau, Yikuan Shi, "Trusted Blockchain-Based Signcryption Protocol and Data Management for Authentication and Authorization in VANETs", Wireless Communications and Mobile Computing, vol. 2022, Article ID 9572992, 14 pages, 2022. https://doi.org/10.1155/2022/9572992

[12]Talha Ahsan, Farrukh Zeeshan khan, Zeshan Iqbal, Muneer Ahmed, Roobaea Alroobaea, Abdullah M. Baqasah, Ihsan Ali, Muhammad Ahsan Raza, "IoT Devices, User Authentication, and Data Management in a Secure, Validated Manner through the Blockchain System", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8570064, 13 pages, 2022. https://doi.org/10.1155/2022/8570064