Journal of Technology Informatics and Engineering (JTIE)
Vol. 3 No. 2 August 2024
E-ISSN: 2987-9434; P-ISSN : 2988-0343, Pages 249-262

A Robust Authentication Method for Electronic Banking Transactions: Two-Way Challenge-Response Approach

Unang Achlison*[1], Miftahurrohman[1], Edy Siswanto[1]
Email: unang@stekom.ac.id, miftah@stekom.ac.id, edy@stekom.ac.id
Orcid: 0000-0001-6295-3446, 0000-0002-7603-5977, 0009-0009-0141-2609
[1]*University of Science and Computer Technology*
*Corresponding Author

Abstract
The security of electronic banking transactions is becoming increasingly critical due to the rising threat of cyberattacks, which can result in financial and reputational damage to financial institutions. Despite the implementation of various authentication methods, vulnerabilities remain that can be exploited by attackers, particularly in the context of static passwords and tokens. This study aims to address these shortcomings by implementing the Two-Way Challenge-Response method, which offers a more robust and dynamic authentication approach. The method employed in this research involves the exchange of information between the client and server, where the challenges generated are unique to each authentication session. This process not only validates user identities but also ensures that the transmitted information cannot be predicted by third parties. The results of the study indicate that the application of this method significantly reduces the risk of attacks such as identity theft and replay attacks, while also enhancing the speed and efficiency of the authentication process. The implications of these findings suggest that the Two-Way Challenge-Response method can be an effective solution for enhancing the security of electronic banking transactions. By adopting this method, financial institutions can strengthen their security systems, increase user trust, and reduce the potential for losses due to cyberattacks. This research contributes significantly to the development of more secure authentication systems in the digital age.

Keywords: *Two-Way Challenge-Response, Electronic Transaction Security, Dynamic Authentication, Electronic Banking, Cyber Attacks.*

I. INTRODUCTION

The rapid growth of electronic banking has revolutionized financial transactions for individuals and businesses alike (Ahmad et al., 2024; Jameaba, 2024). However, this growth has also introduced new security challenges, as cybercriminals increasingly target online banking platforms through phishing, malware, and unauthorized access (Deora, 2021). The rising frequency and sophistication of these attacks underscore the urgent need for stronger authentication mechanisms to safeguard sensitive information. To address these security concerns, financial institutions have adopted various authentication techniques (Bodepudi & Reddy, 2020; Tsai & Su, 2021). Traditional methods, such as passwords and PINs, often fall short due to their susceptibility to attacks (Safder, 2024). Although two-factor authentication (2FA) enhances security by combining something the user knows (e.g., a password) with something they possess (e.g., a device), it is not without limitations. For instance, users remain vulnerable to social engineering attacks or device compromise (Kulkarni & Nath, 2024; Zewdie et al., 2022.

Received on July 09, 2024; Revised on July 30, 2024; Accepted on August 11, 2024. Published on August 21, 2024.
Doi: 10.51903/jtie.v3i2.189.195

Given the dynamic nature of cyber threats, it is crucial to develop more advanced authentication methods that can effectively counter these risks (Hasan et al., 2022; Sarkar & Singh, 2020). This paper introduces a Two-Way Challenge-Response authentication method tailored for electronic banking transactions. This approach not only bolsters security but also prioritizes user convenience—an essential factor for widespread adoption. This study evaluates the effectiveness of the Two-Way Challenge-Response method in mitigating prevalent cyber threats in electronic banking. By comparing it with existing authentication techniques, this research aims to demonstrate the advantages of the proposed method in enhancing online transaction security.

II. LITERATURE REVIEW

A. *Implementation of Authentication*

Authentication is a crucial process in security systems aimed at verifying the identity of users or systems accessing specific services or data. The primary goal of authentication is to ensure that the entity attempting to access the resources is legitimate and authorized to do so. This process has become increasingly important in the context of information and communication technology to protect data and systems from unauthorized access (Joshi et al., 2021; Lone et al., 2020; Rao & Deebak, 2023). Various authentication methods are employed to enhance access security, including password-based authentication, which requires users to enter a pre-registered password. The security of this method heavily relies on the complexity and secrecy of the password used. Additionally, Two-Factor Authentication (2FA) enhances security by requiring two distinct forms of authentication, such as a combination of a password and a code sent to a mobile phone. Biometric authentication, which utilizes physical or behavioral traits such as fingerprints or facial recognition, offers a high level of security due to its unique and difficult-to-forge nature. Token-based authentication involves physical devices or applications that generate unique codes at regular intervals, which must be entered along with other information to gain access.

Certificate-based authentication uses digital certificates issued by a Certificate Authority (CA) to verify identities through public keys and associated information of the certificate holder, securing communications and transactions. Finally, challenge-response authentication involves an interaction between the user and the system, where the system sends a challenge that must be answered with a correct response, typically using algorithms known only to both parties (Hayashi & Ruggiero, 2020; Usman et al., 2022). The implementation of robust authentication methods is essential for maintaining data integrity and confidentiality and building user trust in the systems they utilize (Hasan et al., 2024; Jose Diaz Rivera et al., 2024; Wanisha et al., 2024).

B. Client

In the context of business and information technology, a client is an individual or entity that receives services or products from a service provider. In the business world, this term often refers to customers who utilize professional services such as consultants, lawyers, or insurance agents. In software development and information technology, a client refers to a device or application that interacts with a server to request and receive data or services (Acharya, 2024; Omotayo & Efuntade, 2021). Clients can be individuals using services for personal purposes, companies or organizations requiring products or services for business operations, or government agencies utilizing services to support governmental functions. In a client-server architecture, the client serves as the end user who interacts with applications or services through a user interface. Client Relationship Management (CRM) is a strategy employed to manage interactions between a company and its current and potential clients, to enhance client satisfaction and loyalty through improved and personalized services. It is crucial to understand the needs, preferences, and behaviors of clients so that service providers can develop effective marketing strategies, tailor products or services to meet client expectations and improve service quality while fostering long-term, mutually beneficial relationships (Addimando, 2023; Astuti, 2023; Liladhar Rane et al., 2022; Medaduwe Hewa, 2024; Sihombing & Dinus, 2024).

C. Banking

Banking plays a crucial role in the economy by managing money and providing financial services to individuals, businesses, and governments. Banks serve as intermediaries between savers with excess funds and borrowers in need of capital Buchory & Ekuitas, 2023). The primary services offered by banks include accepting deposits in the form of checking accounts, savings accounts, and term deposits, as well as providing loans for purposes such as home purchases or business capital. Banks also facilitate money transfers between accounts, payments through credit or debit cards, investment, and wealth management services, and foreign exchange services for international trade and travel (Dr. S. BHUVANESWARI, 2023; Long & Pressman, 2024; Sirakova-Yordanova, 2024). Banking plays a crucial role in maintaining economic stability through liquidity management and credit provision, with oversight from central banks to ensure a healthy financial system (Emini1, 2024; Farkhodjon &#38; Dsc, 2024). With technological advancements, digital banking has increasingly developed, allowing customers to access services via the Internet and mobile applications, thereby enhancing the convenience and efficiency of banking services.

D. Electronic Transaction

Electronic transactions refer to the processes of buying and selling conducted via the Internet or other electronic systems (Lambi & Siswani, 2024; Patharia & Jain, 2024; Zarkasi et al., 2024), where buyers and sellers do not interact face-to-face but use electronic devices for activities such as ordering, payment, and delivery of goods or services. This process involves several critical stages: the buyer searches for products or services through an online platform enters personal information and payment details to complete the purchase and receives transaction confirmation. The seller then processes the order based on the received notification. Security in electronic transactions is paramount, with the use of technologies such as data encryption and user authentication to protect personal and financial information. Regulations and standards set by governmental and relevant organizations also play a role in ensuring the security and trustworthiness of electronic transactions (MMhlmann, 2016; Zarkasi et al., 2024). Technological advancements have made electronic transactions increasingly popular, offering convenience and ease for users while enabling sellers to reach customers across various parts of the world (Kolyandov, 2021; Setiawan et al., 2022).

III. RESEARCH METHOD(S)

A. Two-Way Challenge-Response Method

Metode Two-Way Challenge-Response merupakan teknik autentikasi yang dirancang untuk meningkatkan keamanan dalam transaksi elektronik dengan mengimplementasikan pertukaran informasi dinamis antara pihak yang meminta akses (klien) dan pihak yang memberikan akses (server). Metode ini melibatkan proses dua langkah yang terdiri dari pengiriman tantangan (challenge) dan pemberian respons (response), di mana kedua pihak harus saling memvalidasi satu sama lain untuk memastikan identitas dan otorisasi yang sah.

B. Implementation Processes

a. Challenge and Response Exchange

In the initial phase of implementing the Two-Way Challenge-Response method, the server will issue a challenge to the client. This challenge consists of a request for credential information or an authentication code that must be responded to by the client. The client then processes the challenge and sends a valid response back to the server. This response contains information that corresponds to the received challenge or an authentication code generated using an algorithm known only to both parties (Hasan et al., 2024; Kizza, 2024).

b. Identity Verification and Authorization

Upon receiving the response from the client, the server will verify its validity. This verification process ensures that the client requesting access is a legitimate entity and has the right to access the requested resources or services. The verification is performed by comparing the received response with the information generated by the system at the time the challenge was issued (Barrett et al., 2021; Queille & Sifakis, 1982).

c. Security Aspects

The Two-Way Challenge-Response method adds an extra layer of security by ensuring that the authentication process does not rely solely on a single method, such as a password or token, but also requires additional information exchange between both parties. The generated challenges are dynamic or unique for each request, which significantly enhances security and reduces the risk of attacks such as identity theft or replay attacks (Butcher et al., 2007; Zibaeirad et al., 2024).

d. Application in the Context of Electronic Banking

In the context of electronic banking, the Two-Way Challenge-Response method is implemented to ensure the security of financial transactions. This implementation includes the use of dynamic authentication tokens, One-Time Password (OTP) codes, and other authentication protocols that require a specific response known only to authorized parties (Kokila & Reddy K, 2025; Mandava & Dinne, 2010). This method is anticipated to protect the system from security threats and enhance user confidence in electronic banking services.

C. Testing and Evaluation

To measure the effectiveness of the Two-Way Challenge-Response method in the context of electronic banking, a series of tests were conducted, which included:

1. Security Testing: Analyzing the method's resilience against various types of attacks, such as man-in-the-middle and replay attacks.
2. Performance Testing: Evaluating the speed and efficiency of the authentication process in real-world environments to ensure no significant degradation in user experience.
3. User Testing: Collecting feedback from users regarding the usability and satisfaction with the implemented authentication system.
4. The results of these tests are expected to provide insights into the effectiveness of the Two-Way Challenge-Response method in enhancing the security and efficiency of electronic banking transactions, as well as offer recommendations for further development. (Butcher et al., 2007; Kokila & Reddy K, 2025; Mandava & Dinne, 2010; Zibaeirad et al., 2024).

IV. RESULT/FINDINGS AND DISCUSSION

A. Implementation of the Two-Way Challenge-Response Protocol in Web Transactions

This study implements the Two-Way Challenge-Response protocol in the context of web-based electronic banking transactions. In the authentication process, there are two primary entities: the bank customer as the client and the bank as the authentication server (Ahmed et al., 2023; Mohsen & Shaltout, 2023; San Martino & Perramon, 2008). The authentication procedure involves several crucial steps. First, the customer requests access through the bank's application or website. Subsequently, the bank server sends a challenge to the customer, which may involve requesting specific credentials or an authentication code. The customer then responds to the challenge with the requested information or code. The bank server verifies the received response to ensure that the customer accessing the service is a legitimate entity. If verification is successful, access to the electronic banking services is granted to the customer.

This process is crucial for maintaining the security of electronic transactions by ensuring that only authenticated customers can access services and perform transactions. The bank server employs a method where, each time a client logs in, the server generates and sends a randomly generated decimal challenge. This challenge changes dynamically with each login attempt, preventing hackers from rec (Butcher et al., 2007; Zibaeirad et al., 2024). The security principle used is the One-Time Pad, which prioritizes the use of one-time keys for information security. Figure 1 illustrates the use case diagram depicting the implementation of electronic banking transactions, as well as the Level 1 data flow diagram representing the 'challenge-response' protocol.

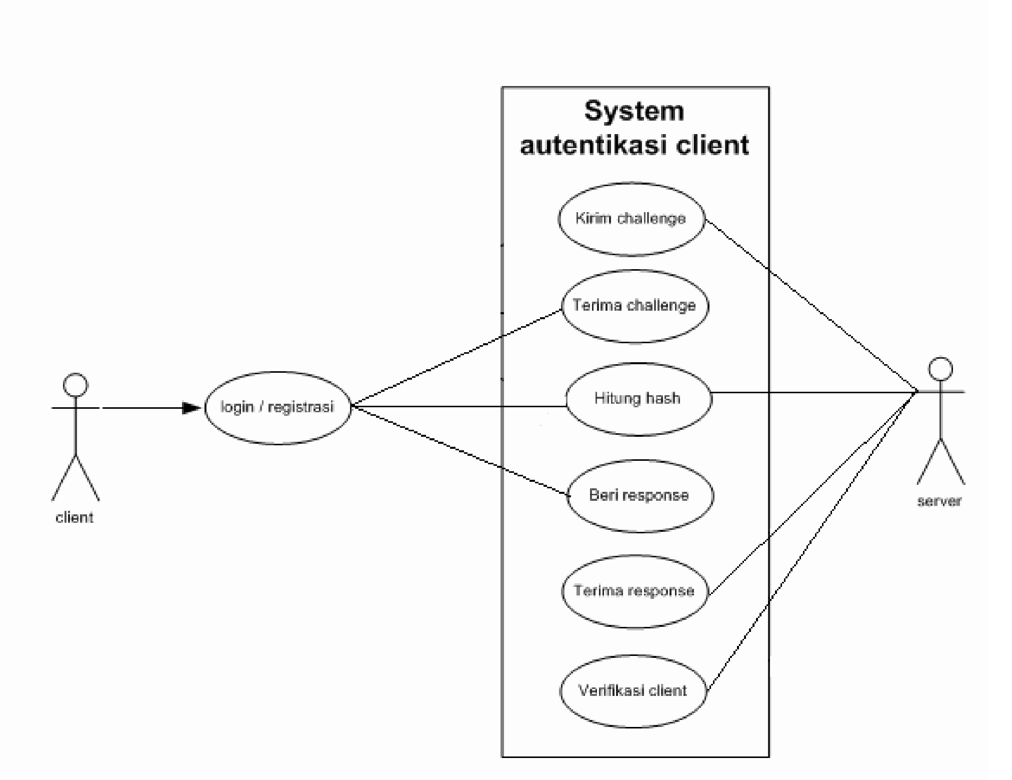


Figure 1. Use Case Diagram of Electronic Banking Transaction Implementation.

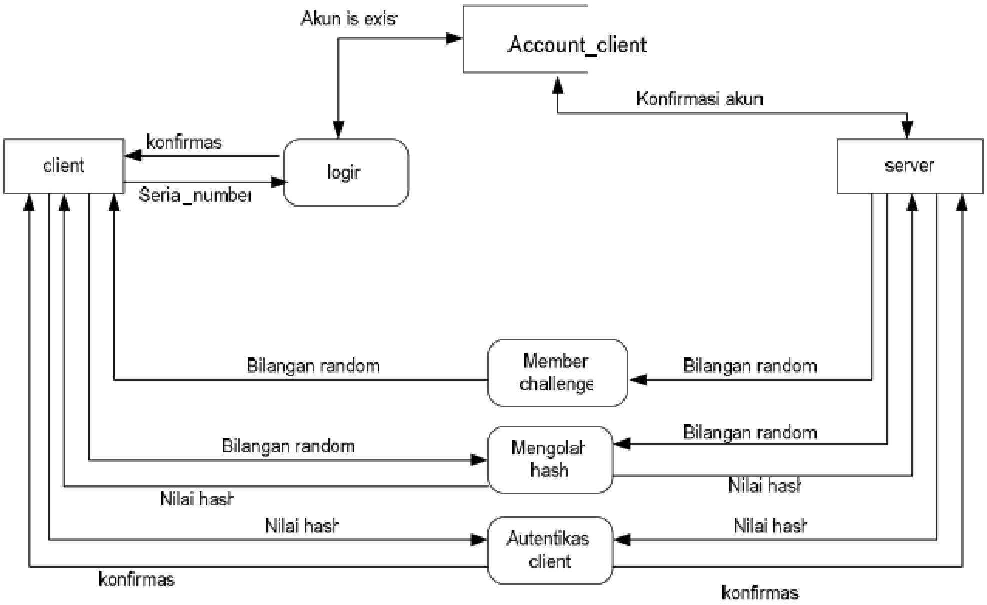
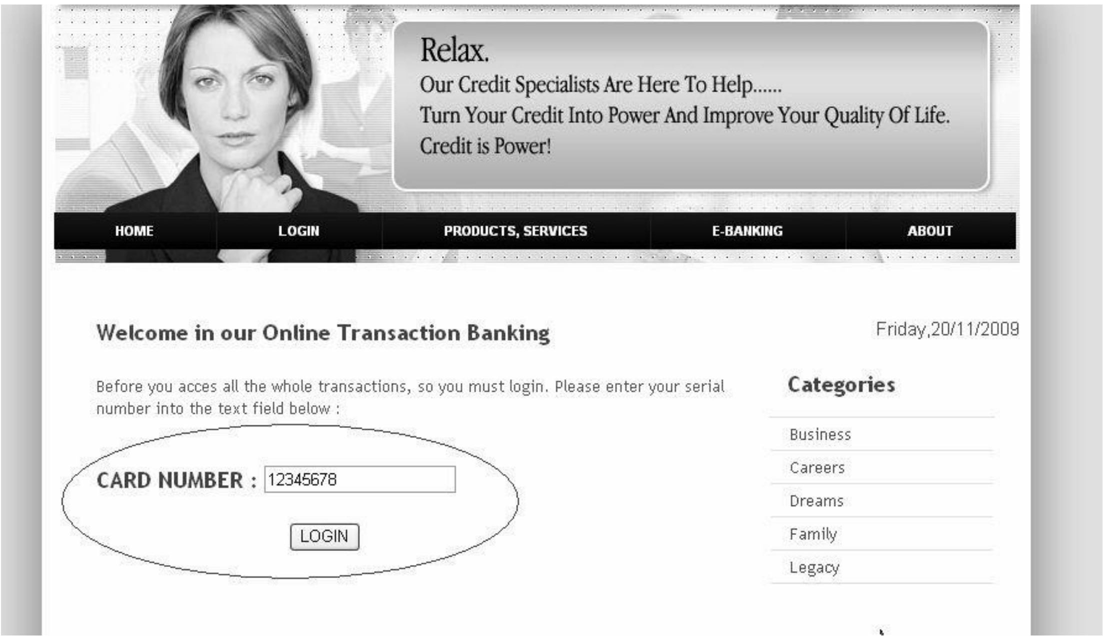


Figure 2. Level 1 Data Flow Diagram of the 'Challenge-Response' Protocol.

The web application interfaces on the server and client during the login process can be observed in Figures 3 and 4. Meanwhile, the hash calculator application running on the client side to generate the hash value of the received challenge can be seen in Figure 5.



Relax.
Our Credit Specialists Are Here To Help......
Turn Your Credit Into Power And Improve Your Quality Of Life.
Credit is Power!

Welcome in our Online Transaction Banking

Friday,20/11/2009

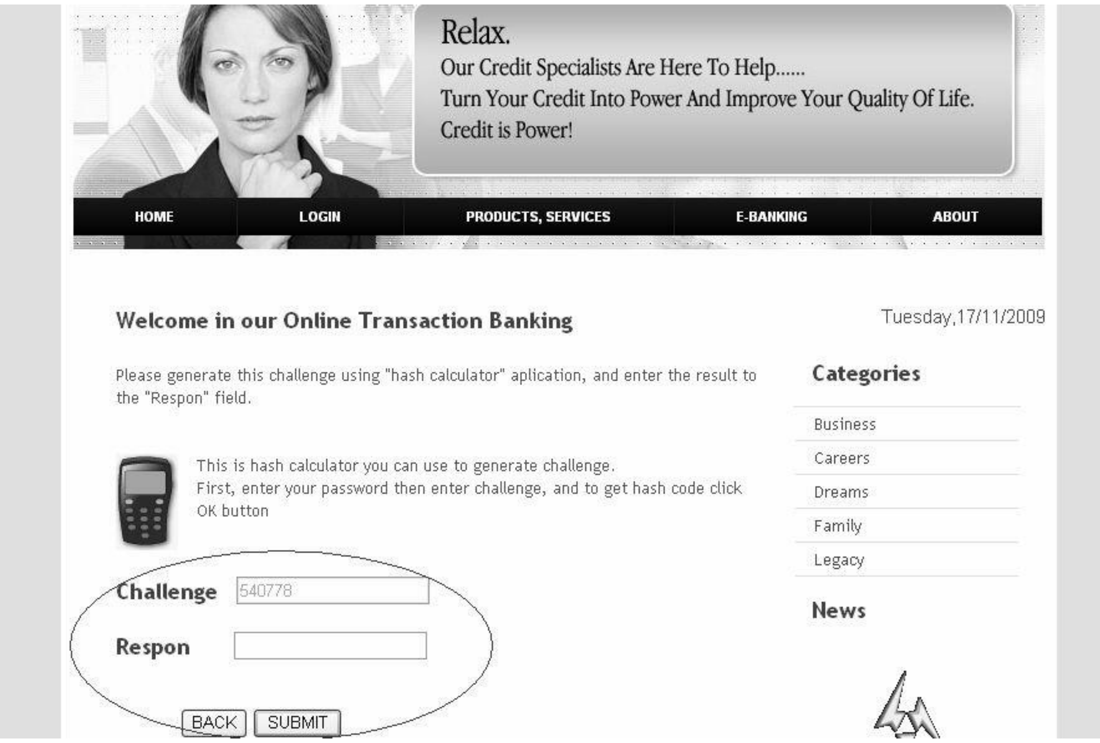
Before you acces all the whole transactions, so you must login. Please enter your serial number into the text field below :

CARD NUMBER : 12345678

Categories

Business
Careers
Dreams
Family
Legacy

Figure 3. Login Web Page on the Server.



Relax.
Our Credit Specialists Are Here To Help......
Turn Your Credit Into Power And Improve Your Quality Of Life.
Credit is Power!

Welcome in our Online Transaction Banking

Tuesday,17/11/2009

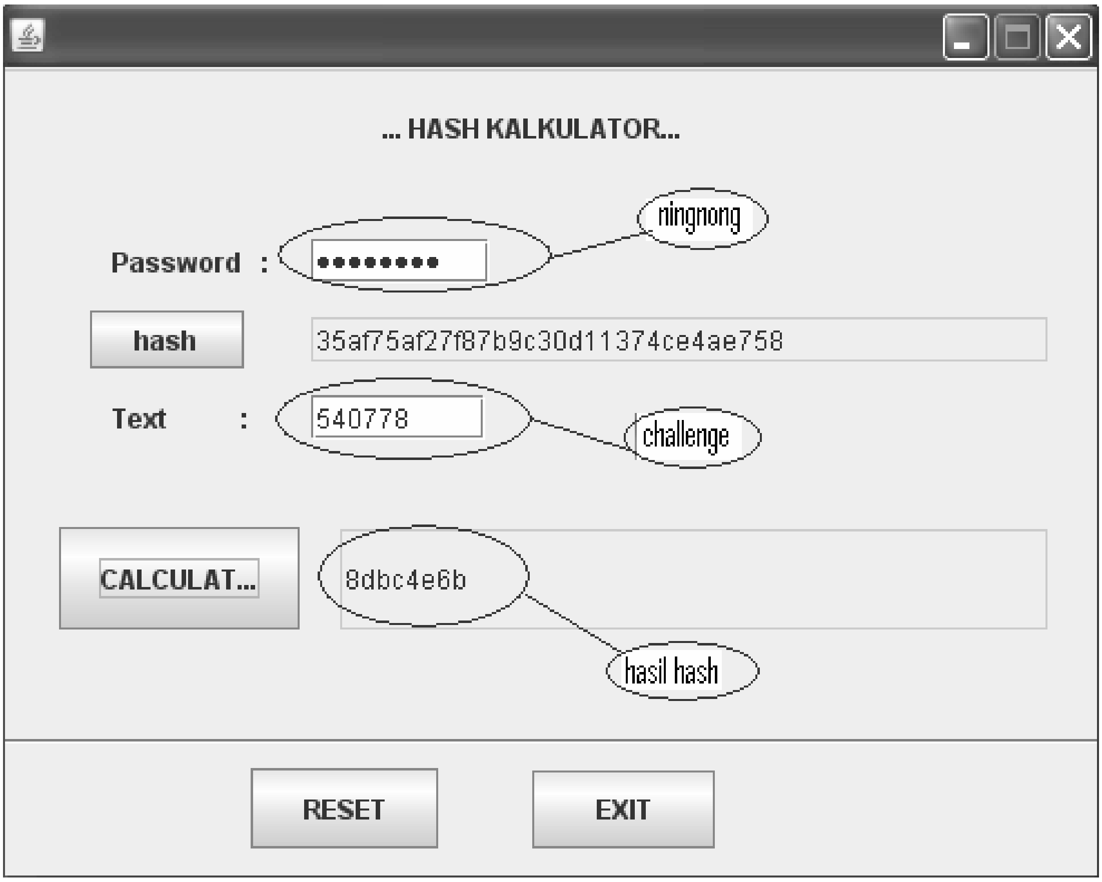
Please generate this challenge using "hash calculator" aplication, and enter the result to the "Respon" field.

This is hash calculator you can use to generate challenge.
First, enter your password then enter challenge, and to get hash code click OK button

Challenge 540778

Respon

Figure 4. Web Page Containing the Challenge.



... HASH KALKULATOR...

Password : ●●●●●●●●●

hash 35af75af27f87b9c30d11374ce4ae758

Text : 540778

CALCULAT... 8dbc4e6b

Figure 5. Hash Calculator Application on the Client.

B. Cryptanalysis of the Two-Way Challenge-Response Protocol

Cryptanalysis of the Two-Way Challenge-Response protocol involves an in-depth analysis aimed at understanding or compromising the security of the protocol by identifying potential weaknesses. Aspects analyzed include the search for challenge patterns, where efforts are made to identify patterns or algorithms used in the generation of challenges by the server. Predictable patterns may create vulnerabilities for replay attacks or structured attacks. Response analysis evaluates how the client's response is generated and authorized by the server, to determine whether there are methods to generate a valid response without knowledge of the specific challenge.

Additionally, cryptanalysis also evaluates the protocol's strength against computational attacks, such as brute-force attacks, and examines the adequacy of the cryptographic algorithms employed. The evaluation is conducted to ensure that the algorithms in use are sufficiently robust to protect sensitive information from cryptanalytic attacks (Butcher et al., 2007; Kokila & Reddy K, 2025; Mandava & Dinne, 2010; Zibaeirad et al., 2024). Testing of various attack schemes is performed to assess the effectiveness and security of the protocol under different conditions. As part of the analysis, testing is conducted on the avalanche effect of the MD5 hash function, which demonstrates MD5's resilience to birthday attacks. The table below presents the results of the avalanche effect test.

Table I

Avalanche Effect Testing on MD5

Sample Input text	Hash code
TI_USD	05776ccd
TI_USD	1328b5dd
TI_USD	4589433d

This test examines the absolute uniqueness of each hash code generated by MD5 for every input text. The birthday paradox, where the probability of two messages having the same hash code increases with the number of hashed messages, is often considered in cryptography to illustrate potential risks in brute-force or exhaustive key space attacks.

V. CONCLUSION AND RECOMMENDATION

The Two-Way Challenge-Response method is an effective authentication approach for enhancing the security of electronic transactions, particularly in the context of banking. By implementing a dynamic information exchange process between the client and server, this method not only ensures legitimate identity and authorization but also adds a significant additional layer of security. The stringent verification process and the use of unique challenges for each request drastically reduce the risk of attacks such as identity theft and replay attacks. Furthermore, this research highlights that the application of robust authentication methods is crucial for maintaining data integrity and confidentiality, as well as for building user trust in the systems they use. Therefore, adopting the Two-Way Challenge-Response method can be a strategic step in addressing security challenges in the continuously evolving digital era.

Building upon the findings of this study, several avenues for future research are recommended to enhance the understanding and application of the Two-Way Challenge-Response authentication method in electronic banking. It is essential to conduct longitudinal studies to assess the long-term effectiveness and user acceptance of this method in various banking environments, which can provide insights into evolving user behavior and perceptions in response to emerging cyber threats. Additionally, exploring the integration of artificial intelligence and machine learning algorithms with the Two-Way Challenge-Response method could lead to the development of adaptive authentication systems that dynamically adjust security measures based on real-time threat assessments and user behavior patterns.

Further research should also include comparative studies evaluating the Two-Way Challenge-Response method against other advanced authentication techniques, such as biometric authentication or blockchain-based solutions. These comparisons can help identify the strengths and weaknesses of each method, guiding financial institutions in selecting the most appropriate security measures. Finally, investigating the implications of regulatory frameworks and compliance requirements on the implementation of the Two-Way Challenge-Response method will be crucial for ensuring that financial institutions can safeguard sensitive information while adhering to legal standards. These research directions will contribute to the development of robust security measures to address the evolving landscape of cyber threats in electronic banking.

REFERENCES

Acharya, K. (2024). Chat Application Through Client Server Management System Project. Chat Application Through Client Server Management System Project. https://doi.org/10.22541/au.172228527.74316529/v1

Addimando, F. (2023). Client-Centered Business Consulting. https://doi.org/10.1007/978-3-031-42844-9

Ahmad, A. Y. A. B., Abusaimeh, H., Rababah, A., Alqsass, M., Al-Olima, N. H., & Hamdan, M. N. (2024). Assessment of effects in advances of accounting technologies on quality financial reports in Jordanian public sector. Uncertain Supply Chain Management, 12(1), 133–142. https://doi.org/10.5267/J.USCM.2023.10.011

Ahmed, K. A. M. ; Saraya, S. F. ; Wanis, J. F. ; Ali-Eldin, A. M. T. A., Gritti, C., Chaudet, C., Ahmed, K. A. M., Saraya, S. F., Wanis, J. F., & Ali-Eldin, A. M. T. (2023). A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards. Future Internet 2023, Vol. 15, Page 208, 15(6), 208. https://doi.org/10.3390/FI15060208

Astuti, S. (2023). Customer Satisfaction Analysis Reviewed From The Perspective Of Services In Tailoring Fund Gede Tembilahan: Analisis Kepuasan Pelanggan Ditinjau Dari Perspektif Pelayanan Jasa Pada Penjahit Pondo Gede Tembilahan. Jumpe (Jurnal Manajemen Pemasaran), 1(3), 112–125. https://doi.org/10.11591/jumpe.v99i1.paperID

Barrett, D., Mazzuchi, T., & Sarkani, S. (2021). A quantitative comparison of the effects of modeling approaches on system verification using a controlled challenge problem. Requirements Engineering, 26(4), 557–580. https://doi.org/10.1007/S00766-021-00358-0/METRICS

Bodepudi, A., & Reddy, M. (2020). Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review. International Journal of Information and Cybersecurity, 4(1), 1–18.

Buchory, H. A., & Ekuitas, S. (2023). GATR Journal of Finance and Banking Review Banking Profitability: How do the banking intermediary, secondary reserve, operational efficiency, and credit risk affect? Article in GATR Journal of Finance and Banking Review, 8(2), 85–96. https://doi.org/10.35609/jfbr.2023.8.2(1)

Butcher, D., Li, X., & Guo, J. (2007). Security challenge and defense in VoIP infrastructures. IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews, 37(6), 1152–1162. https://doi.org/10.1109/TSMCC.2007.905853

Deora, R. S. (2021). Brief Study of Cybercrime on the Internet. https://doi.org/10.37591/JoCES

Dr. S. BHUVANESWARI, Dr. S. C. (2023). “Banking Services of New Generation Banking in the Indian Banking Sector.” Journal of Survey in Fisheries Sciences, 10(2S), 1334–1342. https://doi.org/10.17762/SFS.V10I2S.868

Emini1, F. (2024). The primary focus is on its financial stability. Transnational Academic Journal of Economics, 1(2), 85–94. https://doi.org/10.5281/ZENODO.10884111

Farkhodjon, K., & Dsc, K. (2024). Current Analysis and Current Issues of Ensuring the Financial Stability of the Banking System in Uzbekistan. European Journal Of Business Startups And Open Society, 4(3), 169–176. https://inovatus.es/index.php/ejbsos/article/view/2681

Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., Abdel-Khalek, S., & Alkhassawneh, H. M. (2022). A review of security threats, vulnerabilities, and countermeasures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421–432. https://doi.org/10.1049/CMU2.12301

Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. IEEE Access, 12, 61642–61666. https://doi.org/10.1109/ACCESS.2024.3393567

Hayashi, V., & Ruggiero, W. (2020). Non-Invasive Challenge Response Authentication for Voice Transactions with Smart Home Behavior. Sensors 2020, Vol. 20, Page 6563, 20(22), 6563. https://doi.org/10.3390/S20226563

Jameaba, M.-S. (2024). Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Sector and Beyond. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.4808469

Jose Diaz Rivera, J., Muhammad, A., & Song, W. C. (2024). Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor

Authentication. IEEE Open Journal of the Communications Society, 5, 2792–2814. https://doi.org/10.1109/OJCOMS.2024.3391728

Joshi, S., Stalin, S., Shukla, P. K., Shukla, P. K., Bhatt, R., Bhadoria, R. S., & Tiwari, B. (2021). Unified Authentication and Access Control for Future Mobile Communication-Based Lightweight IoT Systems Using Blockchain. Wireless Communications and Mobile Computing, 2021(1), 8621230. https://doi.org/10.1155/2021/8621230

Kizza, J. M. (2024). Authentication. 215–238. https://doi.org/10.1007/978-3-031-47549-8_10

Kokila, M., & Reddy K, S. (2025). Authentication, access control and scalability models in Internet of Things Security–A review. Cyber Security and Applications, 3, 100057. https://doi.org/10.1016/J.CSA.2024.100057

Kolyandov, S. (2021). The Rising Popularity Of Digital Transaction Platforms. Article in Trakia Journal of Sciences. https://doi.org/10.15547/tjs.2021.s.01.018

Kulkarni, A. V., & Nath, S. (2024). Human Susceptibility to Social Engineering Attacks: an innovative approach to social change. 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2024. https://doi.org/10.1109/IATMSI60426.2024.10502492

Lambi, M., & Siswani, C. B. (2024). Legal Protection For Consumers In Electronic Transactions. Eduvest - Journal of Universal Studies, 4(1), 243–252. https://doi.org/10.59188/EDUVEST.V4I1.1018

Liladhar Rane, N., Achari, A., & Choudhary, S. P. (2020). Enhancing Customer Loyalty Through Quality Of Service: Effective Strategies To Improve Customer Satisfaction, Experience, Relationship, And Engagement. Www.Irjmets.Com @International Research Journal of Modernization in Engineering, 427. https://doi.org/10.56726/IRJMETS38104

Lone, T. A., Rashid, A., Gupta, S., Gupta, S. K., Rao, D. S., Najim, M., Srivastava, A., Kumar, A., Umrao, L. S., & Singhal, A. (2020). Securing communication by attribute-based authentication in HetNet is used for medical applications. Eurasip Journal on Wireless Communications and Networking, 2020(1), 1–21. https://doi.org/10.1186/S13638-020-01759-5

Long, M. G., & Pressman, S. (2024). Postal banking and US cash transfer programs: a solution to insufficient financial infrastructure? Review of Social Economy, 82(2), 213–240. https://doi.org/10.1080/00346764.2023.2259362

Mandava, K., & Dinner, H. (2010). Two Way Mobile Authentication System. https://urn.kb.se/resolve?urn=urn:nbn:se:bth-4306

Medaduwe Hewa, L. (2024). Development of an Effective Marketing Strategy for a Language Institute: understanding customer requirements and behavior.

MMhlmann, M. (2016). Digital Trust and Peer-to-Peer Collaborative Consumption Platforms: A Mediation Analysis. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.2813367

Mohsen, S., & Shaltout, A. (2023). Legal Aspects on the Use of AI in Digital Identity and Authentication in banks, its Impact on the Digital Payment Process A research for investigating the Adaptation of Open Banking Concepts in Egypt By.

Omotayo, E. O., & Efuntade, A. O. (2021). Application Programming Interface (API) And Management of Web-Based Accounting Information System (AIS): Security of Transaction

Processing System, General Ledger and Financial Rep. https://doi.org/10.56201/jafm.v9.no6.2023.pg1.18

Patharia, I., & Jain, T. (2024). Antecedents of Electronic Shopping Cart Abandonment during Online Purchase Process. Business Perspectives and Research, 12(3), 400–418. https://doi.org/10.1177/22785337221148810

Queille, J. P., & Sifakis, J. (1982). Specification and verification of concurrent systems in CESAR. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 137 LNCS, 337–351. https://doi.org/10.1007/3-540-11494-7_22

Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks, 146, 103159. https://doi.org/10.1016

Safder, W. (2024). Password Security, An Analysis Of Authentication Methods.

San Martino, A., & Perramon, X. (2008). A model for securing E-banking authentication process: Antiphishing approach. Proceedings - 2008 IEEE Congress on Services, SERVICES 2008, PART 1, 251–254. https://doi.org/10.1109/SERVICES-1.2008.32

Sarkar, A., & Singh, B. K. (2020). A review on performance,security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37–38), 27721–27776. https://doi.org/10.1007/S11042-020-09197-7/METRICS

Setiawan, A., Nailul Muna, A., Arumi, E. R., & Sukmasetya, P. (2022). The Growth Electronic Commerce Technology and User Interface in Indonesia. Retrieved August 16, 2024, from https://www.researchgate.net/publication/342328542

Sihombing, L., & Dinus, H. (2024). Analysis of Business Development Strategies in Increasing Customer Trust. Journal on Economics, Management and Business Technology, 2(2), 84–92.

Sirakova-Yordanova, G. (2024). Banks Go Beyond Banking: The Expansion Towards Non-Banking Services. https://doi.org/10.2478/picbe-2024-0034

Tsai, C. H., & Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. Information Systems and E-Business Management, 19(1), 77–105. https://doi.org/10.1007/S10257-020-00481-5

Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography. Electronics 2022, Vol. 11, Page 1026, 11(7), 1026. https://doi.org/10.3390

Wanisha, I., James, J. B., Witeno, J. S., Bakery, L. H. M., Samuel, M., & Faisal, M. (2024). Multi-Factor Authentication Using Blockchain: Enhancing Privacy, Security and Usability. International Journal of Computer Technology and Science, 1(3), 41–55. https://doi.org/10.62951/IJCTS.V1I3.24

Zarkasi, M., Hariyanto, E., Asemanis Dua, J., Tokol, L., Pamekasan, K., & Timur, J. (2024). Cash on Delivery Payment System in Online Buying and Selling Perspective of Sharia Economic Law. Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan, 8(1), 121–132. https://doi.org/10.29300/MZN.V8I1.2704

Zewdie, M. T., Girma, A., & Sitote, T. M. (2022). A Comprehensive Review of Insider Threats and Social Engineering Attacks Detection: Challenges, Gaps, and a Deep Learning-Based Solution. https://doi.org/10.2139/SSRN.4766984

Zibaeirad, A., Koleini, F., Bi, S., Hou, T., & Wang, T. (2024). A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities. https://arxiv.org/abs/2407.07966v1