https://dx.doi.org/10.4314/dujopas.v10i3c.30
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 10 No. 3c September 2024*

Comparative Analysis of Remote User Authentication Schemes Based on External Memory

**Bello A. Buhari[1*], Afolayan A. Obiniyi[2],
Sahalu B. Junaidu[2], Armand F. Donfack Kana[2]**

[1]Department of Computer Science,
Usmanu Danfodiyo University,
Sokoto,
Nigeria.

[2]Department of Computer Science,
Ahmadu Bello University,
Zaria,
Nigeria.

Email : buhari.bello@udusok.edu.ng

Abstract

Because of recent availability of remote services and resources, remote user authentication becomes an essential component of all digital environment. Remote user login authentication is the process of validating the identity of a user. Users present their credentials, such as username and password, as evidence of their identity. The most practical and effectively implemented remote user authentication scheme is the smart card-based one, however, because it is expensive to acquire and operate smart card facilities, users may find it challenging to employ smart card authentication schemes in remote environments. Mobility and simplicity of acquisition – especially for remote access – are the benefits of using this external memory. Therefore, this research performs comparative analysis of these remote user authentication schemes based external memory. The schemes are first evaluated for security features and performance in terms of computation cost. The results of analysis shown that Buhari et al.'s scheme has the highest security feature and is the only scheme that uses light-weight tamper resistance client file, followed the reviewed Kumari et al.'s scheme which is the only scheme that handles user privacy. The most efficient scheme is Buhari et al.'s scheme followed by Rhee et al.'s scheme.

Keywords: Remote User, Authentication, External Memory, Security, Computation Cost

INTRODUCTION

Because of recent availability of remote services and resources, remote user authentication becomes an essential component of all digital environment. These include web-based and social media web applications that have features to make it easier for users to access remote applications, share data and can be synchronized with user's Smartphone or Computer (Anwar and Supriyanto, 2019).

Remote user login authentication is the process of validating the identity of a user. Users present their credentials, such as username and password, as evidence of their identity. This will enable them to quickly and easily login to a whole array of other web and remote services (Patel et al., 2022; Buhari and Obiniyi, 2022). Actually, authentication just confirms that users

Author for Correspondence

are who they say they are—it makes no determination as to which entity should be allowed access. Accordingly, users won't be able to access resources based on their stated rights until they have successfully authenticated.

The most practical and effectively implemented remote user authentication scheme is the smart card-based one, which is based on the user's right to access resources based on their defined privileges. The primary security feature of smart cards is their ability to withstand tampering. Other benefits include their small physical size, portability, and the convenience of non-volatile memory. (Buhari et al., 2022). In addition, it is a physical card with an embedded chip that functions as a security token. Additionally, according to Sharma and Dixit (2018), it is a defensive token with an integrated chip that contains information encoded in it.

However, because it is expensive to acquire and operate smart card facilities, users may find it challenging to employ smart card authentication schemes in remote environments (Buhari et al., 2023). This involves setting up the infrastructure required for smart cards and using a method to upload various secure access modules (SAMs) into card readers. Its limited application, such as in financial transactions, arises from this.

An external memory file, on the other hand, is a continuous logical address space that is mapped onto physical devices by the operating system. On an external memory device, it is a designated place used to hold relevant data. Mobility and simplicity of acquisition—especially for remote access—are the benefits of using this external memory (Buhari et al., 2022).

The first remote user authentication scheme based external memory is Rhee et al. (2009). They review existing smart card schemes and found that they cannot directly be converted to scheme using on external memory, therefore, proposed mechanisms to create remote user authentication scheme based on external memory. Then, Chen et al. (2012) proposed a secure password based remote user authentication and key agreement scheme that guarantees mutual authentication and also resists off-line dictionary, replay, forgery, and impersonation attacks. Cryptanalysis of Chen et al. (2012) has been conducted by He et al. (2013). They found out that it is vulnerable to device stolen attack, privileged insider attack, does not provide perfect forward secrecy and no key control, and proposed an improved scheme to resolve these limitations. Jiang et al. (2013) also found that Chen et al. (2012) scheme is insecure against off-line dictionary attack and therefore proposed an enhanced scheme to overcome the limitation. Again, Kumari et al. (2014) found that Jiang et al. (2013) scheme overlooked user's privacy and is vulnerable to insider attack and denial of service attacks, and lacks forward secrecy. Also, He et al. (2013) overlooked user's privacy and change password facility is equivalent to undergoing registration. They therefore, designed a new scheme with user anonymity to resolve the identified weaknesses. Since 2014 there is no research based external memory which may be because of the fact that file in an external memory is not tamper resistance (Buhari et al., 2022). In 2023, Buhari et al. (2023) proposed a light-weight tamper resistant client file in an external memory for remote user authentication and access control. They found that Kumari et al. (2014) is not tamper resistance, not efficient and vulnerable to impersonation attack. They formulated techniques and characteristics that will make client file in an external memory to exhibit light-weight tamper resistance property.

In their comparative research of contemporary IoT security, Dargaoui et al. (2024) provided an analysis of recent authentication schemes in the domains of smart cities, healthcare, industry, etc., spanning the years 2019 to 2023. Bals (2022) examined authentication protocols, namely the multi-factor authentication utilized in the Internet of Things. Using a multi-criteria classification, Azizah and Setiawan (2020) compared various schemes proposed by several researchers and provided a general explanation of the criteria for devices used in smart home environments. The user authentication strategies for real-time data in wireless sensor networks were thoroughly surveyed by Singh et al. (2020), who also conducted a comparison study of these schemes based on security features, communication, user computation, base station computation, and sensor node computation cost. A thorough literature review of recently published academic publications (N = 623) with a primary focus on MFA technologies was conducted by Das et al. (2019). A summary of the latest research on biometric authentication in cloud computing can be found in Alsultan et al. (2019). To decide on the best course of action, they outlined the benefits and drawbacks. A comprehensive overview of the many different IoT authentication schemes that have been proposed in the literature is given by El-Hajj et al. (2019).

In their comparison of authentication techniques, Komarova et al. (2018) used a range of approach criteria, such as usability, performance, security, and other aspects, as well as basic and sophisticated techniques including biometrics and cryptography. In their analysis, Mittal et al. (2018) found that access control protocols and methods of authentication used in wireless sensor networks are more expensive in terms of message exchange and security. The study conducted by Reddy and Reddy (2018) involved a comparative analysis of different multi-factor authentication mechanisms. They provided details on the existing multi-factor authentication mechanisms, including their functionality, applications, locations, and reasons for use. In order to compile existing authentication approaches that have been offered in the literature as well as methods for comparing and choosing them in various settings, Velásquez et al. (2018) conducted a thorough literature study. There are 442 multi-factor authentication methods and 515 single-factor authentication methods in all. In order to provide safe authenticated access to the Telecare Medical Information System, Aslam et al. (2017) examined many authentication methods and discussed their advantages and disadvantages in terms of computing cost, security, and privacy. In order to assess and determine which authentication protocol—such as key management protocols, lightweight authentication protocols, and broadcast authentication protocols—is best for all secure transmission applications in wireless sensor networks, Rajeswari and Seenivasagam (2016) conducted a survey.

Therefore, this research performs comparative analysis of these remote user authentication schemes based external memory. The schemes are first evaluated for security features including anonymity, key distribution resistance, replay attack resistance, impersonation attack resistance, providing mutual authentication, password guessing attack resistance, stolen external memory attack resistance, man-in-the-middle attack resistance, insider attack resistance, denial of service attack resistance, perfect forward secrecy and tamper resistance. Also, they are evaluated for performance in terms of computation cost.

The contributions of this research are as follows:

1. Remote user authentication schemes based on external memory are thoroughly reviewed in order to identify their strengths and weaknesses.
2. The security features evaluation of the schemes is presented with security index in order to identify the most secure and least secure scheme.
3. The performance of the schemes is analysed in terms of computation cost in order to identify the most efficient and least efficient scheme.

The remaining sections of this research are presented as follows: section two is the methodology, section three is the analysis of remote user authentication schemes based on external memory, section four is security analysis of the remote user authentication schemes based on external memory, section five is performance analysis of the remote user authentication schemes based external memory, section six is the conclusion, then acknowledgment and references.

METHODOLOGY

In this research area, a systematic literature review is conducted. First, the review plan is completed, from which the research needs and schemes to be reviewed are obtained. Next, the research papers are categorized so that papers published in the same year are grouped together. Finally, a general search is conducted and duplicate papers are removed to obtain the list of really useful papers. Finally, a detailed analysis of the obtained papers is completed, yielding a list of valuable papers for this research. Then the details on the performance metric in terms of computation cost and security feature that are employed are presented.

Security Features

Security feature is a collection of functions used to protect the connected device from unauthorized use or disclosure of data. The notations used for the analysis of security features of the schemes under study are F1 – Anonymity, F2 – Key distribution resistance, F3 – Replay attack resistance, F4 – Impersonation attack resistance, F5 – Providing mutual authentication, F6 – Password guessing attack resistance, F7 – Stolen external memory attack resistance, F8 – Man-in-the-middle attack resistance, F9 – Insider attack resistance, F10 – Denial of Service attack resistance, F11 – Perfect forward secrecy, F12 – Tamper resistance.

Computation Cost

The overall computing cost is determined by the amount of time a scheme uses for processing and transferring data The notations to be use in the analysis and evaluation of the schemes under study are (Kilinc and Yanik 2013): t_h (One way hash function) – 23ms, t_{Sym} (Cost for symmetric encryption/decryption) – 4.60ms, t_{exp} (Cost of modular exponentiation) – 3850ms and t_{Grg} (Cost of generator and random number on Z_q^*) – 539ms. But xor and concatenation operations are considered negligible.

ANALYSIS OF REMOTE USER AUTHENTICATION SCHEMES BASED ON EXTERNAL MEMORY

In 2009, Rhee et al. first presented a workable and safe user authentication scheme that maintains all the benefits of smart card-based schemes while allowing the usage of a common storage device. The Diffie-Hellman discrete logarithm problem, hash function, and time stamp provide the foundation for its security. Even when a user uses an insecure device, it is safe from off-line dictionary attacks and user and server impersonation attacks. There are three phases to it: the registration, login, and authentication phases. A security study of the Fan et al. (2005) and Rhee et al. (2009) password authentication techniques is carried out by Tan (2009). They concluded that middle man and impersonation attacks might compromise the approach of Rhee et al. So, an attacker could impersonate legitimate users to login and access the remote server.

Another secure password-based remote user authentication scheme without smart cards was developed by Chen et al. (2012). It addresses the issue of user impersonation attacks by including a blind factor into the authentication data kept on the user's local memory device. The computational Diffie-Hellman problem, blind factor, hash function, and time-stamp provide the scheme's security. In addition to providing reciprocal authentication, their suggested technique prevents off-line dictionary, replay, forgery, and impersonation attacks. All of the benefits of the Rhee et al. (2009) scheme is still present. Compared to earlier schemes, there is a decrease in computing cost and a reduced overall message length. This technique is divided into three phases: registration, login, authentication, and password changing.

In their analysis of Chen et al.'s (2012) scheme, Jiang et al. (2013) proposed an enhanced password-based remote user authentication scheme that does not require a smart card. They noted that the approach proposed by Chen et al. is vulnerable to offline dictionary attacks. The hash function and computational Diffie-Hellman problem provide the scheme's security. They showed that the scheme accomplishes mutual authentication between the user and the server and can endure a variety of attacks. In terms of computing and transmission costs, it is more efficient. The initialization phase, registration phase, login and authentication phase, and password changing activity are the three phases that make up their scheme.

He et al. (2013) also conducted cryptanalysis on Chen et al. (2012)'s scheme and discovered that it is susceptible to privilege insider attacks and device theft. Furthermore, it does not allow absolute forward secrecy and no key control. As a result, they proposed an enhanced scheme to address these issues and preserve the advantages of the first scheme. Nevertheless, the approach of Chen et al. (2012) performs better than theirs. Their scheme's security relies on a hash function and the Diffie-Hellman discrete logarithm issue. Phases one through three include registration, login, and authentication.

Jiang et al. (2013) and He et al. (2013) schemes ignore a user's privacy, according to Kumari et al. (2014). They also noted that the Jiang et al. (2013) scheme lacks forward secrecy and is susceptible to denial of service and insider attacks. Additionally, they discovered that while the password-changing feature in He et al. (2013)'s scheme is appropriate, it is inappropriate in Jiang et al. (2013)'s scheme. Once more, neither of the schemes' login phases can stop users from entering the incorrect password, which results in an invalid login request. To address the founded vulnerabilities, they therefore create a new system that protects user anonymity. Additionally, they provided a formal verification of the proposed scheme's security based on the Burrows, Abadi, and Needham logic (BAN logic). It inherits the ability to freely change passwords from Jiang et al.'s schemes, resistance to insider attacks and denial of service attacks from Heet al.'s scheme, etc. Furthermore, it safeguards the identity of the user by granting them anonymity. Initialization, registration, login, authentication, and password change phases are its five stages.

Buhari et al. (2023) proposed a lightweight tamper resistant client file in an external memory as an alternative to smart card for remote user authentication and access control. They reviewed characteristics and design considerations that make smart card tamper resistant. They formulated techniques and characteristics to make a client file in an external memory to exhibit a lightweight tamper resistant property. They also reviewed Kumari et al.’s scheme, which is the latest research that uses external memory for remote user authentication. They presented and modelled the basic system design and software design of the proposed client file. This will enable implementation of the proposed system using any prepared programming or scripting language of one’s choice. Their proposed scheme and reviewed scheme are also evaluated for efficiency, tamper resistance, and impersonation attack. The result of their analysis shown that their proposed scheme is efficient and more secure than the reviewed scheme.

SECURITY ANALYSIS OF REMOTE USER AUTHENTICATION SCHEMES BASED ON EXTERNAL MEMORY

We presented security features analysis of the remote user authentication schemes in this section. The summary of the reviewed remote user authentication schemes based on external memory can be seen in table 1.

Table 1: Summary of reviewed Remote User Authentication Schemes using external memory

Scheme & References	Security Backgrounds	Phases	Limitations
Rhee *et al.* (2009)	Diffie-Hellman discrete logarithm problem, hash function and external memory	Registration, login and authentication	Vulnerable to impersonation attacks and middle man attacks. and not tamper resistance
Chen *et al.*, (2012)	Diffie-Hellman discrete logarithm problem, addition of blind factor, hash function and external memory	Registration, login, authentication and password change	insecure against off-line dictionary attacks, device stolen attack and privilege insider attack, does not support perfect forward secrecy and no key control, and not tamper resistance
Jiang *et al.* (2013)	Diffie-Hellman discrete logarithm problem, hash function and external memory	Initialization, registration, login and authentication, and password change	overlook a user's privacy, vulnerable to insider attack and denial of service attacks, lacks forward secrecy, password change is unsuitable and incapable of preventing the use of wrong password and not tamper resistance
He *et al.* (2013)	Diffie-Hellman discrete logarithm problem, hash function and external memory	Registration, login, authentication and password change	overlook a user's privacy, password changing facility is equivalent to undergoing registration and incapable of preventing the use of wrong password, and not tamper resistance
Kumari *et al.* (2014)	Diffie-Hellman discrete logarithm problem, asymmetric cryptography, hash function, timestamp and external memory	Initialization, registration, login, authentication and password change	user impersonation attack and not tamper resistance
Buhari *et al.* (2023)	Symmetric cryptography, timestamp and light-weight tamper resistance file in an external memory	Registration, login authentication and access control	Key distribution problem and user privacy

The security backgrounds of Rhee et al. (2009) scheme are Diffie-Hellman discrete logarithm, hash function and external memory; Chen et al. (2012) are Diffie-Hellman discrete logarithm, addition of blind factor, hash function and external memory; Jiang et (2013) are Diffie-Hellman discrete logarithm problem, hash function and external memory; He et al. (2013) are Diffie-Hellman discrete logarithm problem, hash function and external memory; Kumari et al. (2014) are Diffie-Hellman discrete logarithm, asymmetric cryptography, hash function, timestamp and external memory and Buhari et al. (2023) are Symmetric cryptography, timestamp and light-weight tamper resistance file in an external memory.

The phases of Rhee et al. (2009) are three namely: registration, login and authentication phases; Chen et al (2012) are four namely: registration, login, authentication and change password phases; Jiang et al. (2013) are four namely: initialization, registration, login and authentication, and change password phases; He et al. (2013) are four namely: registration, login, authentication and change password phases; Kumari et al. (2014) are five namely: initialization, registration, login, authentication and change password phases and Buhari et al. (2023) are three namely: registration, login authentication and access control.

The limitations of Rhee et al. (2009) are vulnerable to impersonation attacks and middle man attacks. and not tamper resistance; Chen et al. (2012) are insecure against off-line dictionary attacks, device stolen attack and privilege insider attack, does not support perfect forward secrecy and no key control, and not tamper resistance; Jiang et al. (2013) are overlook a user's privacy, vulnerable to insider attack and denial of service attacks, lacks forward secrecy, password change is unsuitable and incapable of preventing the use of wrong password and not tamper resistance; He et al. (2013) are overlook a user's privacy, password changing facility is equivalent to undergoing registration and incapable of preventing the use of wrong password, and not tamper resistance; Kumari et al. (2014) are user impersonation attack and not tamper resistance and Buhari et al. (2023) are key distribution problem and user privacy.

Table 2: Security features of the remote user authentication schemes based on external memory

Scheme	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	Security Index
Rhee *et al.* **(2009)**		✓	✓		✓								3
Chen *et al.*, **(2012)**		✓	✓		✓								3
Jiang *et al.* **(2013)**		✓	✓		✓				✓				4
He *et al.* **(2013)**		✓	✓		✓				✓	✓	✓		6
Kumari *et al.* **(2014)**	✓	✓	✓		✓	✓			✓	✓	✓		8
Buhari *et al.* **(2023)**			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10

Buhari et al. (2023) has the highest number of security features with security index of 10 and is the only scheme that used tamper resistance client file in an external memory, followed by Kumari et al. (2014) with security index of 8 and is the only scheme with anonymity features. He et al. (2013) has security index of 6, Jiang et al. (2013) has security index of 4 and both Chen et al. (2012) and Rhee et al. (2009) has security index of 3.

PERFORMANCE ANALYSIS OF REMOTE USER AUTHENTICATION SCHEMES BASED ON EXTERNAL MEMORY

We presented performance analysis of the remote user authentication schemes in this section. Computation cost of the schemes under study will be analysed and compared.

Computation Cost Analysis

According to table 3, the computation cost of Rhee et al. (2009) is $2t_{Grg} + 5t_h$which is equivalent to 1193ms, Chen et al. (2012) is $10t_h + 2t_{Grg} + 4t_{Exp}$ which is equivalent to 16708ms, Jiang et al. (2013) is $10t_h + 2t_{Grg} + 4t_{Exp}$ which is 16708ms, He et al. (2013) is $11t_h + 3t_{Grg} + 7t_{Exp}$ which 28820ms, Kumari et al. (2014) is $2t_{Sym} + 4t_{Grg} + 4t_{Exp}$ which is 17565.20ms and Buhari et al. (2023) is $3t_{Sym}$ which is 13.80ms.

Table 3: Computation cost of the remote user authentication using based on external memory

Scheme	Computation Cost	Computation Time (ms)
Rhee *et al.* (2009)	$2t_{Grg} + 5t_h$	1193
Chen *et al.*, (2012)	$10t_h + 2t_{Grg} + 4t_{Exp}$	16708
Jiang *et al.* (2013)	$10t_h + 2t_{Grg} + 4t_{Exp}$	16708
He *et al.* (2013)	$11t_h + 3t_{Grg} + 7t_{Exp}$	28820
Kumari *et al.* (2014)	$2t_{Sym} + 4t_{Grg} + 4t_{Exp}$	17565.20
Buhari *et al.* (2023)	$3t_{Sym}$	13.80

From table 3, Buhari et al. (2023) is more efficient, followed by Rhee et al. (2009). Chen et al. (2012) and Jiang et al. (2013) has the same computation cost and He et al. (2013) has the highest computation cost. This can be shown in figure 1.

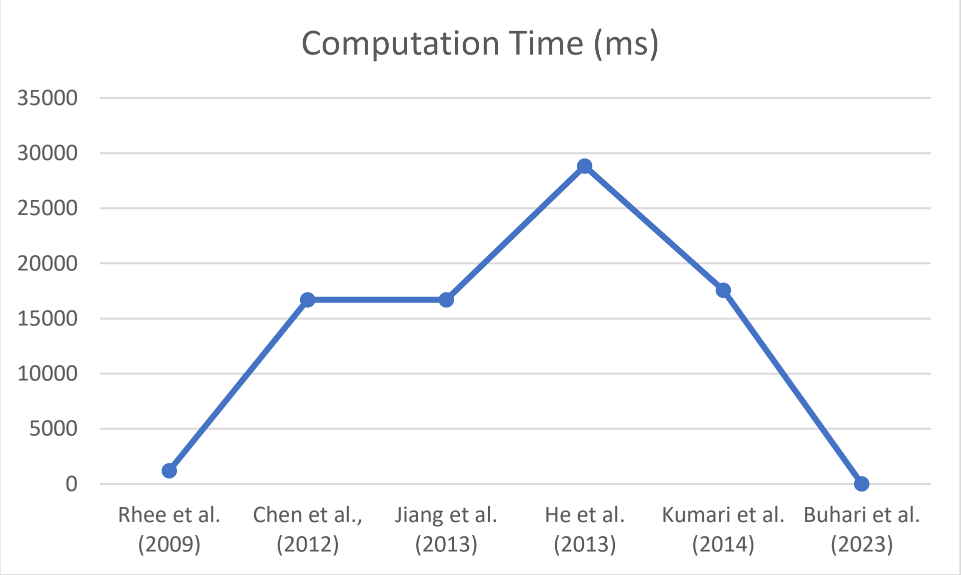

Figure 1: Comparison of computation cost.

CONCLUSION

Based on a user's stated privileges and their ability to access resources, the smart card-based remote user authentication technique is the most practical and well-executed. However, users may find it difficult to use smart card authentication techniques in remote contexts due to the high cost of acquiring and maintaining smart card facilities. The advantages of adopting this external memory include its mobility and ease of acquisition, particularly for distant access. This study does a comparative examination of different external memory-based remote user authentication systems. The first step in evaluating the schemes' security features is to determine whether they are anonymous, resistant to key distribution, replay attacks, impersonation attacks, mutual authentication, password guessing attacks, attacks involving stolen external memory, resistant to man-in-the-middle attacks, resistant to insider attacks, resistant to denial-of-service attacks, perfect forward secrecy, and resistant to tampering. They are also evaluated based on computation cost. Based on the analysis, Buhari et al. (2023) has the highest security feature count with a security index of 10, and is the only scheme that uses a tamper-resistant client file in an external memory. Kumari et al. (2014) comes in second with a security index of 8, and is the only scheme that has anonymity features. He et al. (2013) has a security index of 6, Jiang et al. (2013) has a security index of 4, Chen et al. (2012) and Rhee et al. (2009) have security index of 3.

AKNOWLEDMENTS

This research was funded by TETFUND under the 2024 Institution Based Research (IBR) Annual Intervention (IBR-UDUS-B8-007), we therefore acknowledge their immense support.

Also, we appreciate Usmanu Danfodiyo University, Sokoto - Nigeria for their infrastructure support.

REFERENCES

Alsultan, T. M., Salam, A. A., Alissa, K. A., & Saqib, N. A. (2019, June). A comparative study of biometric authentication in cloud computing. In *2019 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

Anwar, N., & Supriyanto, S. (2019). Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *8*(3), 206-212.

Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., & Aslam, B. (2017). A survey of authentication schemes in telecare medicine information systems. *Journal of medical systems*, *41*, 1-26.

Azizah, A. N., & Setiawan, F. B. (2020, October). Comparison of Authentication Schemes on IoT. In *2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE)* (pp. 158-162). IEEE.

Bals, J. (2022). *A comparative analysis of the multi-factor authentication protocols presented in the literature* (Bachelor's thesis, University of Twente).

Buhari, B. A., & Obiniyi, A. A. (2022). Web applications login authentication scheme using hybrid cryptography with user anonymity. *Int. J. Inf. Eng. Electron. Bus.(IJIEEB)*, *14*(5), 42-50.

Buhari, B. A., Obiniyi, A. A., Junaidu, S. B., & Kana, A. F. D. (2022). Trends in Remote User Authentication Based on Smart Card and External Memory. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, *14*(1), 1-10.

Buhari, B. A., Obiniyi, A. A., Junaidu, S. B., & Kana, A. F. D. (2023). A Light Weight Temper Resistance Client File in an External Memory for Remote User Authentication and Access Control. *International Journal of Systems and Software Security and Protection (IJSSSP)*, *14*(1), 1-21.

Chen, B. L., Kuo, W. C., & Wuu, L. C. (2012). A secure password-based remote user authentication scheme without smart cards. *Information technology and control*, *41*(1), 53-59.

Dargaoui, S., Azrour, M., El Allaoui, A., Guezzaz, A., Alabdulatif, A., & Alnajim, A. (2024). Internet of Things Authentication Protocols: Comparative Study. *Computers, Materials & Continua*, *79*(1).

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating user perception of multi-factor authentication: A systematic review. *arXiv preprint arXiv:1908.05901*.

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, *19*(5), 1141.

Fan, C. I., Chan, Y. C., & Zhang, Z. K. (2005). Robust remote authentication scheme with smart cards. *Computers & Security*, *24*(8), 619-628.

He, D., Wang, D., & Wu, S. (2013). Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. *Information technology and control*, *42*(2), 105-112.

Jiang, Q., Ma, J., Li, G., & Ma, Z. (2013). An improved password-based remote user authentication protocol without smart cards. *Information technology And control*, *42*(2), 113-123.

Kilinc, H. H., & Yanik, T. (2013). A survey of SIP authentication and key agreement schemes. *IEEE communications surveys & tutorials*, *16*(2), 1005-1023.

Komarova, A., Menshchikov, A., Negols, A., Korobeynikov, A., Gatchin, Y., & Tishukova, N. (2018). Comparison of authentication methods on web resources. In *Proceedings of the*

Second International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'17) Volume 1 (pp. 104-113). Springer International Publishing.

Kumari, S., Khan, M. K., Li, X., & Wu, F. (2014). Design of a user anonymous password authentication scheme without smart card. *International Journal of Communication Systems*, *29*(3), 441-458.

Mittal, V., Gupta, S., & Choudhury, T. (2018). Comparative analysis of authentication and access control protocols against malicious attacks in wireless sensor networks. In *Smart Computing and Informatics: Proceedings of the First International Conference on SCI 2016, Volume 2* (pp. 255-262). Springer Singapore.

Patel, S., Sahoo, A., Mohanta, B. K., Panda, S. S., & Jena, D. (2019, March). DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-5). IEEE.

Rajeswari, S. R., & Seenivasagam, V. (2016). Comparative study on various authentication protocols in wireless sensor networks. *The Scientific World Journal*, *2016*(1), 6854303.

Reddy, B. K. K., & Reddy, B. I. (2018). A comparative analysis of various multifactor authentication mechanisms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(5), 8.

Rhee, H. S., Kwon, J. O., & Lee, D. H. (2009). A remote user authentication scheme without using smart cards. *Computer Standards & Interfaces*, *31*(1), 6-13.

Sharma, Y. K., & Dixit, S. (2018). Smart Card for Healthcare System. *International Journal of Electronics Engineering.*, *10*(1), 359–362.

Singh, D., Kumar, B., Singh, S., & Chand, S. (2020). Evaluating authentication schemes for real-time data in wireless sensor network. *Wireless Personal Communications*, *114*(1), 629-655.

Tan, Z. (2009, June). Security analysis of two password authentication schemes. In *2009 Eighth International Conference on Mobile Business* (pp. 296-300). IEEE.

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30-37.