A Systematic Review on Multi-Factor Authentication Framework

Muhammad Syahreen[1], Noor Hafizah[2], Nurazean Maarop[3], Mayasarah Maslinan[4]
Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia[1, 2, 3]
Information Security Management Assurance, CyberSecurity Malaysia, Kuala Lumpur, Malaysia[1, 4]

***Abstract*—In the new era of technology, where information can be accessed and gained at the push of a button, security concerns are raised about protecting the system and data privacy and confidentiality. Traditional ways of user authentication are vulnerable to multiple attacks across all platforms. Various studies propose the use of more than one authentication process to enhance the security level of a system, either hosted on-premise or on the cloud. However, there is limited study on guidelines and appropriate authentication frameworks that suit the needs of an organization. A systematic literature review of a Multi-Factor Authentication framework was conducted through five primary databases: Scopus, IEEE, Science Direct, Springer Link, and Web of Science. The review examined the proposed solution and the underlying methods in a Multi-Factor Authentication framework. Numerous authentication methods were combined to address specific system and data security challenges. The most common authentication method is biometric authentication, which addresses the uniqueness of the user's biological identity. The majority of the proposed solutions were proof of concept and require a pilot test or experiment in the future.**

***Keywords*—Data privacy; information; multi-factor authentication; security challenges**

I. Introduction

The authentication process is the first defense against unauthorized access, a critical security system component [1]. Authentication is the process of identifying the authorized user to have valid access to a device or system. The authentication process starts by registering a valid user with sufficient information such as username, password, and email address. All the information is stored on the server and will be verified during the login process. The most common authentication methods are text passwords [2], Identification Numbers (PIN) [3], and biometrics [4]. Hence, protecting a system requires a sufficient, reliable, and vigorous authentication framework [5].

Single-factor authentication (SFA) is the most popular authentication method among users and is widely implemented. However, SFA is vulnerable to cyber-attacks because it provides basic security protection. Recent studies reveal the need for multi-factor authentication (MFA) to secure the user's connection to the systems and applications. Many MFA frameworks have been proposed to address the challenges in authentication security. Unfortunately, one framework does not fit all of them. Hence, this study aimed to systematically review the existing MFA framework and the proposed solution.

This systematic review consists of five sections. Section I explicitly covers the introduction and significance of this review. Section II provides a study background on MFA and its challenges. Then, Section III discusses the study methodology and summary of the findings. Section IV highlights the related findings, literature discussion, and presents the comparative analysis of the proposed MFA framework. Finally, Section V concludes the study findings and discusses the potential future research.

II. Related Work

Researchers in the literature have proposed various MFA frameworks to address cyber-attacks. In most recent cases of cyber-attacks on systems and applications, the enhancement of authentication security has been proposed to mitigate the risk. The organization needs authentication security to protect the systems and data confidentiality, privacy, and availability.

Many authentication frameworks have been proposed in the literature to address the weak authentication issue. Every proposed MFA framework has its advantages and disadvantages. Leslie Lamport, in 1981, announced the first remote authentication method based on an encryption function, a one-way hash encryption function, and a password lookup table. However, although the proposed authentication is easy to use, the authentication requires a high hash overhead and more significant storage to store the password databases. Hence, some studies address the use of smart cards to overcome the weakness. For example, [6] presented a scheme combining a smart device and a third-party application to perform a single sign-on authentication in the cloud environment. Several smartcard or smart device methods have been proposed in the literature, particularly [6] and [7].

However, many of the proposed authentication approaches require additional equipment, such as a smart card reader and biometric scanner, for the authentication process. The second category of approaches is digitalized multi-factor authentication. The other proposed authentication framework combines RSA encryption for the digital signature and One-Time Password (OTP), which utilizes asymmetric and RSA digital signature as the second factor [8]. The proposed framework required three phases: setup, user registration, and authentication process. Therefore, the proposed authentication framework does not require devices such as a token device, a smart card system card reader, and a physiological biometrics scanner [9].

A. Authentication Framework

The security and authentication issues of a system or application hosted on-premises or cloud, like NFC hacking, stolen accounts and devices, and insecure access points, can be

alleviated by proper authentication. As the authentication data is stored in a server, user privacy is highly vulnerable to those attacks.

The traditional authentication method relies on a username and password, which is no longer safe and adequate to protect the system on cloud computing. Therefore, Two-Factor Authentication (2FA) was introduced as an intuitive step forward that couples the representative data with the factor of personal ownership, such as a smartcard or a phone. The smartcard device is used as the second authentication factor to strengthen security.

Previous literature argued on the security protection provided by SFA, hence proposing a 2FA framework [2][10][11][12]. 2FA is an authentication mechanism for protecting users from phishing attacks and password leakage [13]. However, various research simultaneously challenges the implementation of the 2FA, which limits the device to the second authentication protocol [14] [15] [16]. In summary, most literature agrees that MFA provides comprehensive security protection to the system environment compared to SSO and 2FA frameworks [17].

Hence, to overcome the challenges in authentication security, an MFA was utilized to secure the system and data ecosystem. MFA combines multiple authentication methods into a sequence of the authentication process. MFA utilized three factors to connect the user with the established credentials:

- Information factor – something that the user knows.
- Ownership factor – something that the user has.
- Biometric factor – something the user is.

Afterward, the MFA framework was introduced to enhance the security protection of a system and facilitate the continuous preservation of computing devices and systems from unauthorized access. The development of an MFA framework required at least two authentication methods, which provide possession, knowledge, and uniqueness [18] [19]. In the MFA framework, username passwords and biometrics are the two most common authentication methods used with other additional authentication [15]. According to industry experts, text passwords, one-time passwords (OTP), and two-factor combinations are the most widely used authentication techniques and approaches. The primary rationale for their selection was that they were suited for the application under development [17].

In addition, mobile environments, healthcare and telecare, wireless sensor networks, remote authentication, cloud computing, and crypto depend on the MFA framework. Therefore, MFA introduced an additional security layer to the system by implementing a time-based one-time password (TOTP) method [20]. The proposed TOTP required a username and password in the first stage. Then, the user needs the MFA token to generate a TOTP virtually. The proposed authentication method is found to provide a secure transaction.

B. Gaps in Authentication Framework

Single authentication is the most basic and convenient protection mechanism using a password-based authentication scheme. Some examples of password-based authentication methods are Automated Teller Machines (ATM), Database Management Systems, and Personal Digital Assistants (PDA). However, two main problems are associated with the password mechanism [21]. First, passwords and PINs are stored in database systems as plain text can easily be accessed by the administrator. Secondly, the attacker can impersonate a legitimate user by grabbing the user ID and password stored in the database.

Therefore, MFA is considered the solution to the various challenges mentioned above. MFA involves a multi-layer authentication scheme to reduce the risks of SFA, such as unauthorized access to trusted devices and modification to the data structure. Previous research on MFA substantially concentrated on the technological improvement of authentication and the limitation of user access control to address existing weaknesses in various areas.

However, technological adoption, usability, and system alignment with user risk perception remain a question [22]. While new authentication methods have been more interesting to explore, previous studies have also intensively evaluated existing MFA frameworks. On the aspect of speed, simplicity (user actions), and authentication error rates on the user side [23] [24] [25]. However, the usability of high-touch and low-tech schemes remains challenging [22].

Despite the industry being a major workforce and data repository source, only 2.4% of the research focused on any MFA organizational implementation [22]. The industrial implication is often understudied, primarily because the data policies of the industry, as well as the lack of contribution from the organizations themselves and the recruitment of the technical expert, can be challenging.

Table I summarizes various studies focusing on the proposed MFA framework from 2016 until 2022.

TABLE I. SUMMARY OF MFA FRAMEWORKS

No	Authentication Method	Author(s), year
1	Text Password	[26]
2	Graphical Password	[27]
3	Biometric	[28] [29]
4	One Time Password (OTP)	[30] [31]
5	Token	[32]
6	Card Reader	[33]
7	Time-based One Time Password (TOTP)	[34]

III. METHODOLOGY

A systematic literature review (SLR) identifies, evaluates, and interprets all available research relevant to a particular research question, topic area, or phenomenon of interest. Most research starts with a conventional literature review to gain input on the selected topic. However, unless a literature review is thorough and fair, it is of little scientific value. This is the primary rationale for undertaking systematic reviews. A SLR synthesizes existing work in a manner that is fair and seems to

be fair. Some of the features that differentiate a systematic review from a conventional expert literature review are:

- Systematic reviews start by defining a review protocol specifying the research question being addressed and the methods used to perform the review.
- Systematic reviews are based on a defined search strategy to detect as much relevant literature as possible.
- Systematic reviews of the selected documents for the search strategy so that readers can assess their rigor and the repeatability and completeness of the entire process.
- Systematic reviews require explicit inclusion and exclusion criteria to assess each potential primary study and the scope of interest.
- Systematic reviews specify the information to be obtained from established databases, including quality criteria by which to evaluate each primary study.
- A systematic review is a prerequisite for quantitative meta-analysis.

SLR plays a vital role in supporting further research efforts and providing an unbiased synthesis and interpretation of the findings in a balanced manner [35]. Fig. 1 below illustrates the SLR overview process.

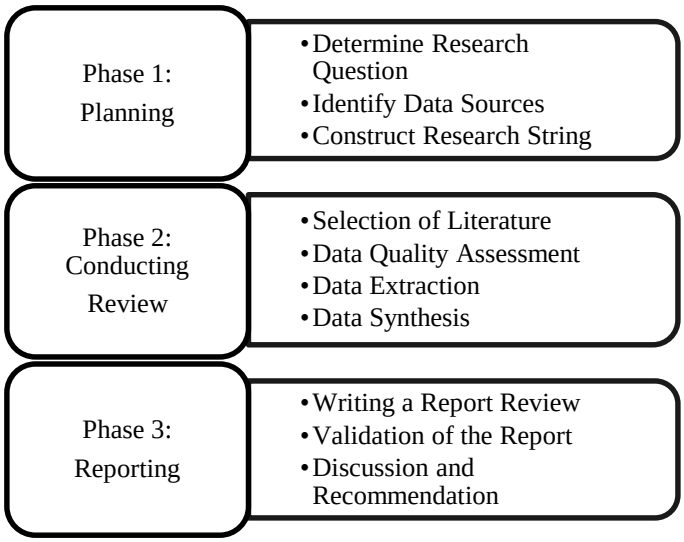

Fig. 1. Overview of the methodology in SLR.

Phase 1 in SLR involved planning the review, including developing research questions, an online sources database, and a research string. This study developed the research questions as follows:

- What is the proposed authentication solution in the study?
- What is the comparison of the proposed authentication methods in the study?

This study identifies suitable online databases [15] [36], which include Scopus, IEEE, Science Direct, Springer Link, and Web of Science (WoS). Google Scholar was used as a secondary data source, and a reverse snowballing technique was used to identify potential research. The search string included ""multi-factor"" OR ""multi-tier"" OR ""multi-layer"" AND ""authentication"" AND ""framework"" OR ""model"". Boolean operators have been applied to refine and broaden the search required. The findings are summarized in Table II. After conducting the search from five databases, a total of 248 papers were found.

The collected papers went through the second phase in SLR to determine the relevant literature by [35] applying seven stages of the filtering process shown in Table III to ensure only related and appropriate literature on multi-factor authentication was discussed. Fig. 2 illustrates the quality assessment stages, and a total of 23 literatures were selected for discussion.

TABLE II. SUMMARY OF RESEARCH FINDINGS

No	Database (DB)	Research Finding
1	Scopus	83
2	IEEE	65
3	Science Direct	23
4	Springer Link	19
5	Web of Science (WoS)	58
TOTAL		248

TABLE III. INCLUSION AND EXCLUSION FILTERING CITERIA

Stage#	Inclusion/exclusion criteria
Stage 1	Searching research papers through the search strings on major online databases to discover conference papers and journal articles.
Stage 2	Excluding research papers, that is non-English papers, a short paper, a poster presentation, slide presentations, editorials, and prefaces.
Stage 3	Removing replicated research paper that appears in different databases
Stage 4	Reading the research paper (the introduction, method section, and conclusion)
Stage 5	Excluding the research paper that was not relevant to authentication method / MFA
Stage#	**Inclusion/exclusion criteria**
Stage 6	Excluding the research paper that did not propose solutions, evaluation, or experience of authentication method / MFA
Stage 7	Excluding the research papers that do not answer two or more of the identified research questions

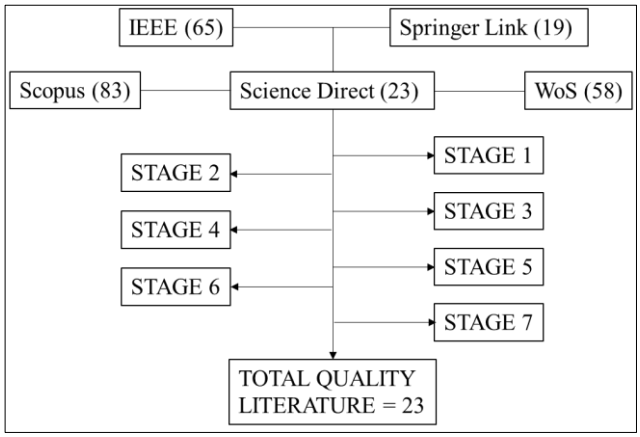

Fig. 2. Quality assessment stages in SLR.

The data extraction strategy is applied to display the selected literature in an organized structure. The criteria of the data extraction strategy were only the relevant literature selected to be reviewed and documented accordingly.

The final stage of SLR involves writing the report by analyzing the result to meet the study objective. The objective of SLR is to identify the proposed multi-factor authentication (RO1) and to compare the proposed authentication methods in the study (RO2).

IV. Results and Discussion

This study has identified 23 relevant literatures on the MFA framework through the SLR process. Table V below summarizes the findings from the SLR process and the proposed authentication methods, where 23 literatures were analyzed based on the proposed authentication methods in the MFA framework.

A. Proposed MFA Framework

The proposed MFA framework comprises ten authentication methods. Each MFA framework utilizes more than one authentication method in the framework. This study discussed the advantages and disadvantages of each proposed authentication method.

1) Biometric authentication: Dynamic signature is one such biometric modality used to authenticate an individual during the establishment of identities [37]. The proposed dynamic signatures utilized structural and behavioral characteristics that are unique to the user during the signing process. The dynamic signature requires a special digital surface, such as a digitizing tablet and pen, but it is comparatively harder to forge and is claimed to be 99% accurate. Other researchers also discussed and proposed behavioral biometrics [29] [38] [39] [41] [42] [44] [48] [49] as well as deep learning analysis besides multimodal biometric input which combined at least two biometric features [40].

2) One-time password authentication: The authentication method of a one-time password (OTP) provides confidentiality to the users [45]. However, there is a significant challenge to the proposed authentication method where possible masquerade attacks happen to the verification process, and complex protocols with high computational costs may occur. In the current context of OTP, there are many patented OTP tokens, which may be proprietary hardware tokens, application- and software-based OTP, and web-based approaches [31] [41] [43] [53][57].

3) Cryptography authentication: Cryptography or encryption authentication is believed to provide confidentiality and integrity to the system security [44]. Generally, cryptography uses an asymmetric cryptosystem to exchange the secret key and then employ faster secret key algorithms to ensure confidentiality of the data stream. Meanwhile, a symmetric cryptosystem is used to encrypt and decrypt messages using the same secret key. In addition, hash functions are non-public key cryptography and work without a key. Various literature has been proposed to enhance the authentication framework through cryptography [29]. Traditional encryption is used in block and stream ciphers to guarantee the confidentiality of the data. The advanced encryption method, such as Transport Layer Security (TLS), is used in securing communication. The proposed authentication method in an MFA framework needs to be integrated with another system or method. Moreover, the system integrator is required to employ cryptography-based protocols through hashing, block ciphers, public keys, and private key generators [44] [31] [29]. Thus, create a complex authentication solution for the MFA framework.

4) Username and password authentication: The proposed authentication through username and password can be considered the pioneer and traditional authentication method, posing significant limitations and vulnerabilities [41]. The variety of password attacks and the huge amount of accessible password leaks and dictionary attacks make it indispensable to find more reliable alternatives. However, with the revolution in security and technologies, many researchers proposed an enhanced way to authentication through username and password, such as encrypting the text, adopting a global namespace, challenge password, dynamic password [37], web password [38], and many others. Despite that, many researchers agree that username and password need to be combined with another authentication method to create a secure authentication process [38] [39] [40] [41].

5) IoT or Smart Device Authentication: The increase in the number of smart Internet of Things (IoT) devices provides additional authentication security. A smart device can be integrated with a user's behavior that is captured from multiple embedded sensors [39]. In addition, smart devices are favored in artificial intelligence (AI) or work as sensors to detect geolocation or GPS coordination. A mobile phone is considered a smart device and can be used to perform biometric identification, push notifications, and installed applications that perform user verification [48] [49].

6) Graphical password authentication: Previous literature has proposed various graphical authentication methods to assess authentication security. The graphical password technique is believed to counter shoulder-surfing attacks during the authentication process [38]. A graphical interface displays a pre-determined object, button, or menu item for the authentic user's action [27]. Graphical passwords can be combined in a series of significant challenge questions to the user.

7) Token-based authentication: A secure token-based system can be dependable as well as non-dependable, and factors that rely on an algorithm for generating the token can be dependable. Token-based authentication is widely used among banking customers for secure financial transactions. A YubiKey hardware token is amongst the top-rated authentication security devices [38]. However, there are high requirements for complex system integration, pre-analyzed and pretested software applications with multiple systems, and additional costs are required to possess the hardware token [42].

8) Dynamic keypad authentication: Pattern-based or dynamic keypad authentication is commonly used during the

registration phase. A block grid with numbers and symbols is given to the user [47]. The key function maps the numbers selected from the grid pattern to the key, providing a more secure password [31]. Smart devices are also used to perform the authentication process but are likely to be manipulated by an adversary by accessing sensitive data by unlocking mobile devices. Moreover, mobile devices and the applications installed are exposed to unauthorized modification and spyware [56].

9) Software or application authentication: Application and system providers utilize third-party application libraries and provide a tested software application for user authentication [42]. A push notification is used to provide the secret key or code to the application installed on a device such as Google and Microsoft Authenticator. This method reduces human error since the user is not required to copy the code. However, most third-party applications and libraries are exposed to security risks such as men-in-the-middle attacks (MITM), hence violating the user's data privacy and confidentiality [42].

10)Email authentication: Email authentication is a technique to prove that the email is not forged and belongs to the authenticated user. Email authentication is most often used with other authentication methods and is not used alone but rather as a medium to transmit the secret code or identify the authorized user [27] [43] [54]. The email address is often used during the registration phase [31] [48]. However, authentication through email can be manipulated using phishing attacks, resulting in unauthorized access to the system. Previous literature discussed this security issue and proposed a secondary authentication layer such as time-based OTP through email, combining a secret word with emailed OTP codes, and many others [48].

B. Discussion on the Selected MFA Framework

This study selected an experiment work by [43] for the discussion in the real-world application as well as the guideline for future research. The study proposed an MFA framework based on TOTP, conventional username and password. The experiment was conducted by registering a user. The system requirement forced the user to enter a strong password with a combination of symbols and numbers. The user needs to verify the account through a valid email sent to ensure the user's validity and to avoid errors during typing.

During the login phase, the user is required to enter the registered username and password. The system verifies the user identity with the password database in encryption mode. Once the process passes, the system will generate a random OTP code and send it to the user's registered email for verification purposes. The valid time for the user to enter the OTP code is within 60 seconds. Fig. 3 below depicts the process flow of the proposed OTP. The experiment was conducted to evaluate the success rate of the proposed solution with different hash functions. Table IV shows the generated average values from the experiment for single hash function computations.

The authentication experiment uses a set TOTP validity of one second to generate the passcode. The value of the parameter underwent thorough testing in the utilized scenarios. The response varies based on the network latency and the hosts' performance in the authentication procedure. In a real environment, the configuration must adhere to the usability requirements of the entire system.

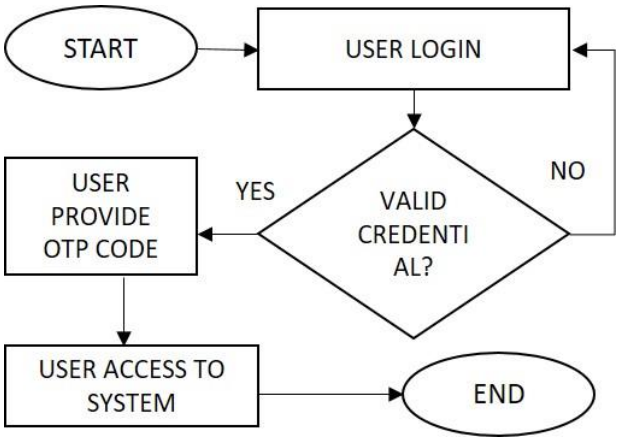

Fig. 3. Quality assessment stages in SLR.

TABLE IV. TIME REQUIRED FOR HASHING COMPUTATION OTP

No	Hash Function	Average Hash Chain (HC) over Hash Value (HV)
1	SHA-256	87 - 99
2	SHA-512	118 - 132
3	SHA3-256	111 - 114
4	SHA3-512	148 - 166

V. CONCLUSION

The weakness of single-factor and two-factor authentication leads to the implementation of MFA and several authentication policies. The application of a multi-factor authentication, intrusion detection mechanism, and user identity access management (IAM) is able to ensure the security and privacy of the data and system. In addition, cryptography through encryption techniques is efficient to protect the data from being disclosed during data in transit and data at rest.

In many cases, the system owners are responsible for ensuring the data's security, privacy, confidentiality, and availability. Adding a second layer of protection after authentication methods such as SSLVPN, IAM, intrusion prevention, and detection ensures the data are well protected.

Conducting a risk assessment to determine the likelihood and level of risk associated with the system and data will ensure adequate preparation and support business as usual (BAU). This study has identified 23 relevant papers on authentication methods in order to propose an MFA framework.

This study believes a comprehensive MFA framework can be developed to benefit users by addressing the challenges and gaps in authentication security. MFA frameworks need to include the three basic authentication factors:

- "Something you know" (such as password).
- "Something you have" (such as a device).
- "Something you are" (such as biometric).

In addition, to ensure end-to-end security protection, the user and system provider should include network security mechanisms such as SSL, TLS, SSLVPN, and user access control such as Identity Access Management (IAM).

However, adopting the correct authentication methods through MFA has significant challenges and limitations. The effectiveness of the proposed MFA structure depends on several factors, such as operational budget, complexity of the system, technical support, system integration, and the availability of mobile networks.

This study reviewed the proposed authentication frameworks through a systematic literature review. In addition, this study also discussed one of the potential MFA frameworks for adoption in the real environment in the previous chapter. The future direction of this study is to integrate the IAM framework and other security features to enhance data protection in the cloud computing environment. IAM ensures that only valid users have access to the resources such as data, records the user login details, and limits or removes user access, including the system administrator.

TABLE V. THE PROPOSED MFA FRAMEWORK AND COMPARATIVE ANALYSIS OF AUTHENTICATION METHODS

No	Author (A)	Proposed Authentication Method									
		Biometric	OTP / TOTP	Cryptography	Username / Password	IoT / Smart Device	Graphical Password	Token-based	Dynamic Keypad / Pattern-key	Software / Application Authenticator	Email
1	[37]	√			√						
2	[38]	√			√		√	√			√
3	[39]	√			√	√					
4	[40]	√			√						
5	[41]	√	√		√	√					
6	[42]	√				√		√		√	
7	[27]				√		√				√
8	[43]		√		√						√
9	[44]	√		√	√						
10	[45]		√		√						
11	[31]		√	√	√				√		
12	[46]		√								
13	[47]		√		√				√		
14	[48]	√			√	√			√		√
15	[49]	√			√	√					
16	[50]		√		√						
17	[51]				√					√	
18	[29]	√		√							
19	[52]	√	√		√						
20	[53]		√		√						
21	[54]				√					√	√
22	[55]		√		√						
23	[56]		√		√				√		√

ACKNOWLEDGMENT

This work was supported/funded by the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS/1/2013/ICT04/UTM/02/1).

REFERENCES

[1] Al Harbi, S., Halabi, T. and Bellaiche, M. (2020) "Fog Computing Security Assessment for Device Authentication in the Internet of Things", in Proceedings - 2020 IEEE 22nd International Conference on High Performance Computing and Communications, IEEE 18th International Conference on Smart City and IEEE 6th International Conference on Data Science and Systems, HPCC-SmartCity-DSS. Institute of Electrical and Electronics Engineers Inc., pp. 1219–1224.

[2] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K. (2019) "A Usability Study of Five Two-Factor Authentication Methods", Fifteenth Symposium on Usable Privacy and Security.

[3]] Guerar, M., Migliardi, M., Palmieri, F., Verderame, L. and Merlo, A. (2020) "Securing PIN-based authentication in smartwatches with just two gestures", Concurrency and Computation: Practice and Experience. John Wiley and Sons Ltd, 32(18).

[4] Alizadeh, M., Dowlatshah, K., Ahmadzadeh Raji, M. and Nabiel Alkhanak, E. (2020) "Coding theory View project User Privacy of Internet of Things View project A secure and robust smart card-based remote user authentication scheme", Article in International Journal of Internet Technology and Secured Transactions, 10(3), pp. 255–267.

[5] Prabhanjan Yadav, B., Shiva Sai Prasad, C., Padmaja, C., Naik Korra, S. and Sudarshan, E. (2020) "A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing", IOP Conf. Series: Materials Science and Engineering, 981.

[6] Karthigaiveni, M. and Indrani, B. (2019) "An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card", Journal of Ambient Intelligence and Humanized Computing. Springer Verlag.

[7] Bouchaala, M., Ghazel, C. and Saidane, L. A. (2022) "Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card", Journal of Supercomputing. Springer, 78(1), pp. 497–522.

[8] Sarna, S. and Czerwinski, R. (2022) "Small prime divisors attack and countermeasure against the rsa-otp algorithm", Electronics (Switzerland) MDPI AG. MDPI, 11(1).

[9] R. Madhusudhan and M. Hegde (2019) "Smart Card Based Remote User Authentication Scheme for Cloud Computing", in IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 905–910.

[10] J. Colnago et al., ""It's Not Actually That Horrible': Exploring Adoption of Two-Factor Authentication at a University," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–11, doi: 10.1145/3173574.3174030.

[11] Li, S., Xu, C., Zhang, Y. and Zhou, J. (2022) 'A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens', IEEE Transactions on Information Forensics and Security, 17, pp. 3525–3538.

[12] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-Factor Authentication for IoT With Location Information," IEEE Internet Things J., vol. 6, no. 2, pp. 3335–3351, 2019, doi: 10.1109/JIOT.2018.2882610.

[13] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-Factor Authentication: Is the World Ready? Quantifying 2FA Adoption," 2015, doi: 10.1145/2751323.2751327.

[14] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018) 'Multi-Factor Authentication: A Survey', in Cryptography, pp. 1–31.

[15] Velásquez, I. (2021) 'Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication', in CLEI ELECTRONIC JOURNAL.

[16] B. W. Kwon, P. K. Sharma, and J. H. Park, "CCTV-based multi-factor authentication system," J. Inf. Process. Syst., vol. 15, no. 4, pp. 904–919, 2019, doi: 10.3745/JIPS.03.0127.

[17] Velásquez, I., Caro, A. and Rodríguez, A. (2018) 'Authentication schemes and methods: A systematic literature review', Information and Software Technology. Elsevier, 94, pp. 30–37.

[18] Singh, C. and Singh, T. (2019) 'A 3-Level Multi-factor Authentication Scheme for Cloud Computing', International Journal of Computer Engineering & Technology (IJCET), 10(1), pp. 184–195.

[19] Karie, N. M., Kebande, V. R., Ikuesan, R. A., Sookhak, M. and Venter, H. S. (2020) 'Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud', PervasiveHealth: Pervasive Computing Technologies for Healthcare. ICST.

[20] Taher, K. A. , Nahar, T. , and Hossain, S. A. , (2019) 'Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm', in International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST). IEEE, pp. 308–312.

[21] Rajasekar, V., Jayapaul, P., Krishnamoorthi, S. and Saračević, M. (2021) Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications: A Multi-layer Systematic Survey, Acta Polytechnica Hungarica.

[22] Das, S., Wang, B., Tingle, Z. and Camp, L. J. (2019) Evaluating User Perception of Multi-Factor Authentication A Systematic Review.

[23] Xiong, W., Zhou, F., Wang, R., Lan, R., Sun, X. and Luo, X. (2018) 'An Efficient and Secure Two-Factor Password Authentication Scheme with Card Reader (Terminal) Verification', IEEE Access. Institute of Electrical and Electronics Engineers Inc., 6, pp. 70707–70719.

[24] Nag, S., Chiat, S., Torgerson, C. & Snowling, M. J. (2014).Literacy, foundation learning and assess-ment in developing countries: final report. (London, EPPI-Centre, Social Science Research Unit,University of London)

[25] Abo-Zahhad, Mohammed, Sabah M. Ahmed, and Sherif N. Abbas. "A new multi-level approach to EEG based human authentication using eye blinking." Pattern Recognition Letters 82 (2016): 216-225.

[26] Bong, J., Suh, Y. and Shin, Y. (2016) 'Fast user authentication method considering mobility in multi clouds', in 2016 International Conference on Information Networking (ICOIN), pp. 445–448.

[27] Meng, W., Zhu, L., Li, W., Han, J. and Li, Y. (2019) Enhancing the security of FinTech applications with map-based graphical password authentication, Future Generation Computing Systems.

[28] Neha and Chatterjee, K. (2019) 'Biometric re-authentication: an approach towards achieving transparency in user authentication', Multimedia Tools and Applications. Springer New York LLC, 78(6), pp. 6679–6700.

[29] Prabhu, D., S. Vijay Bhanu, and S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment." Measurement: Sensors 24 (2022): 100511.

[30] Ma, S., Feng, R., Li, J., Liu, Y., Nepal, S., Ostry, D., Bertino, E., Deng, R. H., Ma, Z. and Jha, S. (2019) 'An empirical study of SMS one-time password authentication in android apps', in ACM International Conference Proceeding Series. Association for Computing Machinery, pp. 339–354.

[31] Gosavi, S. S., & Shyam, G. K. (2021). A novel approach of OTP generation using time-based OTP and randomization techniques. In Data Science and Security: Proceedings of IDSCS 2020 (pp. 159-167). Springer.

[32] Li, S., Xu, C., Zhang, Y. and Zhou, J. (2022) 'A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens', IEEE Transactions on Information Forensics and Security, 17, pp. 3525–3538.

[33] Xiong, W., Zhou, F., Wang, R., Lan, R., Sun, X. and Luo, X. (2018) 'An Efficient and Secure Two-Factor Password Authentication Scheme with Card Reader (Terminal) Verification', IEEE Access. Institute of Electrical and Electronics Engineers Inc., 6, pp. 70707–70719.

[34] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "TOTP Moving Target Defense for sensitive network services," Pervasive Mob. Comput., vol. 74, pp. 0–18, 2021, doi: 10.1016/j.pmcj.2021.101412.

[35] Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering–a tertiary study. Information and software technology, 52(8), 792-805.

[36] Hafiza Razami, H. and Ibrahim, R. (2022) 'Models and constructs to predict students' digital educational games acceptance: A systematic literature review', Telematics and Informatics. Elsevier Ltd, 73.

[37] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAMCloud: a cloud based Mobile biometric authentication framework," Multimed. Tools Appl., vol. 82, no. 25, pp. 39571–39600, 2023, doi: 10.1007/s11042-022-13514-7.

[38] A. Robles-González, P. Arias-Cabarcos, and J. Parra-Arnau, "Privacy-centered authentication: A new framework and analysis," Comput. Secur., vol. 132, 2023, doi: 10.1016/j.cose.2023.103353.

[39] Y. Yang, X. Huang, J. Li, and J. S. Sun, "BubbleMap: Privilege Mapping for Behavior-Based Implicit Authentication Systems," IEEE Trans. Mob. Comput., vol. 22, no. 8, pp. 4548–4562, 2023, doi: 10.1109/TMC.2022.3166454.

[40] J. S. Mane and S. Bhosale, "Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics," Rev. d'Intelligence Artif., vol. 37, no. 3, pp. 709–718, 2023, doi: 10.18280/ria.370319.

[41] Lone, Sajaad Ahmed, and Ajaz Hussain Mir. "A novel OTP based tripartite authentication scheme." International Journal of Pervasive Computing and Communications 18.4 (2022): 437-459.

[42] Ibrokhimov, Sanjar, Kueh Lee Hui, Ahmed Abdulhakim Al-Absi, and Mangal Sain. "Multi-factor authentication in cyber physical system: A state of art survey." In 2019 21st international conference on advanced communication technology (ICACT), pp. 279-284. IEEE, 2019.

[43] Chenchev, I. (2023). Framework for Multi-factor Authentication with Dynamically Generated Passwords. In Future of Information and Communication Conference (pp. 563-576). Cham: Springer Nature Switzerland

[44] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An improved time-based one time password authentication framework for electronic payments. Int. J. Adv. Comput. Sci. Appl, 11(11), 359-366.

[45] Bose, R., Chakraborty, S., & Roy, S. (2019, February). Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors. In 2019 Amity International Conference on Artificial Intelligence (AICAI) (pp. 764-768). IEEE.

[46] Megouache, L., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and information sciences, 10, 1-20.

[47] Phoka, T., Phetsrikran, T., & Massagram, W. (2018, November). Dynamic keypad security system with key order scrambling technique and OTP authentication. In 2018 22nd International Computer Science and Engineering Conference (ICSEC) (pp. 1-4). IEEE.

[48] Yellamma, P., Rajesh, P. S. S., Pradeep, V. V. S. M., & Manishankar, Y. B. (2020). Privacy preserving biometric authentication and identification in cloud computing. Int. J. Adv. Sci. Technol, 29(6), 3087-3096.

[49] Nalajala, S., Moukthika, B., Kaivalya, M., Samyuktha, K., & Pratap, N. L. (2020). Data security in cloud computing using three-factor authentication. In International Conference on Communication, Computing and Electronics Systems: Proceedings of ICCCES 2019 (pp. 343-354). Springer.

[50] Babkin, S., & Epishkina, A. (2019, January). Authentication protocols based on one-time passwords. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 1794-1798). IEEE.

[51] Gordin, I., Graur, A., & Potorac, A. (2019, October). Two-factor authentication framework for private cloud. In 2019 23rd international conference on system theory, control and computing (ICSTCC) (pp. 255-259). IEEE.

[52] Kaur, S., Kaur, G., & Shabaz, M. (2022). A secure two-factor authentication framework in cloud computing. Security and Communication Networks, 2022, 1-9.

[53] Cunha, V. A., Corujo, D., Barraca, J. P., & Aguiar, R. L. (2021). TOTP Moving Target Defense for sensitive network services. Pervasive and Mobile Computing, 74, 101412.

[54] Berrios, J., Mosher, E., Benzo, S., Grajeda, C., & Baggili, I. (2023). Factorizing 2fa: Forensic analysis of two-factor authentication applications. Forensic Science International: Digital Investigation, 45, 301569.

[55] Erdem, E., & Sandıkkaya, M. T. (2018). OTPaaS—One time password as a service. IEEE Transactions on Information Forensics and Security, 14(3), 743-756.

[56] Binbeshr, F., Por, L.Y., Kiah, M.M., Zaidan, A.A. and Imam, M., 2023. Secure pin-entry method using one-time pin (OTP). IEEE Access, 11, pp.18121-18133.

[57] Chenchev, I. (2023). Framework for Multi-factor Authentication with Dynamically Generated Passwords. In Future of Information and Communication Conference (pp. 563-576). Cham: Springer Nature Switzerland.