University of Ibadan
Journal of Science and Logics in ICT Research

Robust Authentication Medium for Safety of Financial Transactions

****Festus-Amaka Eugenia N.[1], Odii, Juliet N.[2], Isa Ali Ibrahim[3], Okolie, Stanley Adiele[4], and Ayogu, Ignatius I.[5]**

**[1, 3] Department of CyberSecurity, School of Information and Communication Technology, Federal University of Technology, Owerri- Nigeria
[2,4 & 5]Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri- Nigeria
**Ngozi.festus-amaka@futo.edu.ng[1], Juliet.odii@futo.edu.ng[2], ibrahim.ali@futo.edu.ng[3], Sokolie@futo.edu.ng[4], Ig.ayogu@gmail.com[5]

** Correspondence

Abstract

The SMS-based authentication medium for financial transaction poses vulnerability challenges on its transmission medium due to weak authentication medium. These security challenges are not limited to various attack mechanisms such as Man in the middle (MITM), replay among others on the transit. Also, the transmission channel of Short Message Service (SMS) via device could be stolen and SMS been transmitted could equally be vulnerable to attacks. Hence, this study develops an International Mobile Equipment Identity (IMEI) Authentication Technique (IAT), to redirect the focus of financial authentication medium to both user and device authentication medium, where both the user and device will be authenticated. Therefore, the study captures the two user authentication mechanisms, in addition to device identity authentication to ensure a secured communication and any attempt of illegitimate processes will be aborted.

Keywords: *Authentication medium, Sensitive information, Transmission medium, Vulnerability, Financial transaction.*

1. INTRODUCTION

The yardstick of attaining a maximum security measure regarding data integrity and reliability among others solely depends on the intensity of the authentication protocol design, which should not be limited to user-involvement alone Kaur and Mustafa [1]. The researchers claimed that users easily compromise their sensitive information. Though, it may seem difficult but not impossible to limit users' roles on the authentication processes, if security challenges will be enhanced. Thus, to successfully achieve this, has been the target of the researchers in proposing the authentication mechanisms for both users and their devices. Hence, to greatly achieve the security design process, this simply means that both the user and the initiating device must effectively be incorporated on the financial authentication protocol design to adequately enhance the security measures. However, there is no doubt that both user and device been incorporated on the authentication medium will extremely perform wonders.

Thus, the security of data-integrity depends on the authentication factors chosen. However, these authentication factors, are chosen from the knowledge-factors of the users, such as PIN, password, username, pattern lock, etc.; possession -factors, such as token, smartcards, etc. and inheritance-factors, which include both the physiological and behavioral biometric features of the users. The physiological biometric features include facial recognition, palm prints, iris recognition

Festus-Amaka Eugenia N., Odii, Juliet N., Isa Ali Ibrahim, Okolie, Stanley Adiele, and Ayogu, Ignatius I. (2023). Robust Authentication Medium for Safety of Financial Transactions, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 10 No. 1, pp. 1 – 8

among others, while the behavioral biometric features are the character exposition of the user such as the way the user walks, talks, reacts to issues among others, Banga and Pillai, [4]; Dadakhanov [5]. Also, the users' choice of authentication is determined by the number of factors required. These factors are Single Factor Authentication (SFA), Two Factor Authentication (TFA/2FA), and Multi-Factor Authentication (MFA).

Therefore, the sensitive information is being generated by combining any of the authentication factors, which is expected to be kept secured, free from any form of compromise, either from user or weak network system. Though, the issue of data security cuts across all approaches to data, such as data in transit, data in process, and data at rest. However, the transmission protocol of data in transit being vulnerable on transitional phase because of SMS-based authentication medium involvement has been a major concern of this research. SMS-based medium is not a secured service for transmitting sensitive information because the security of the data is not assured. Therefore, Papaspirou *et al.* [6], ascertained that National Institute of Standards and Technology (NIST) condemned the use of SMS-based authentication medium, claiming that it works as store and forward, whereby any information stored using SMS could be replicated as many times as possible and equally be forwarded to various destinations.

Furthermore, there are other lots of security implications of using SMS-based protocol which are not limited to fear of uncertainty, such as users' device being stolen and SMS of OTP been transmitted to such device is being intercepted Arif *et al*,. [3]; Papaspirou *et al.* [6]; Ramasamy, *et al.* [8]

To address these security challenges of SMS-based medium, the focus of user authentication mechanisms as implemented in most of the existing research should be enhanced. Also, to achieve this goal, a device layer authentication was design to authenticate the initiating device of the user along with authentication of other user's claimed identities. Thus, this will enable the identification of illegitimate users or devices penetrating to the system.

However, focus-shift from user authentication to device authentication mechanism is an utmost security measure to curb the security challenges faced by many financial institutions, which has rendered the users account to zero. Hence, the device authentication will require the IMEI (International mobile equipment identity) number of the device, device type and the device color for secured security measure. When a request is initiated, the IMEI number of the device that initiated the request will be verified to ensure source authenticity for initiating request.

Despite the shortcomings of the SMS-based authentication protocol, the available research noted that it is a widely used medium in authentication processes for transmitting the generated OTPs. But it is important to address the question that says "who is the end user of the SMS being transmitted on the user's device?" An SMS may have been assumed to have been transmitted to the user without knowing if it is actually the intended user that receives the message or not.

2. LITERATURE REVIEW

It was discovered in a research conducted by Reese *et al.*,[9], that the sensitive information of the users was transmitted to the user's device, which had drawbacks such as delay in delivery, poor network service, and human error to copy the OTP codes from phones to other devices. Also, the researchers admitted that the authentication using SMS-based is vulnerable since messages are not encrypted on transit in any mobile network. This, results to the various attack mechanisms such as Man in the Middle (MITM), phishing, replay, SIM swapping, eavesdropping among others.

lso, Ryu & Kim,[10], in their research transmitted the SMS-based verification code to the users' SIM, inserted on the users' device, requesting for both the behavioural and environmental data of the user, while the user responds by using the same device to send the code to the server and the server sends the authenticated result to the user's device. Thus, the researchers agreed that the SMS-based authentication is vulnerable to various attack mechanisms such as transit attack by MITM,

eavesdropping attack on the verification codes of the users, and smishing, whereby the verification codes of the users are being intercepted through an unintentional installation of the malicious applications by the users.

Furthermore, research conducted by Papaspirou et al., [6], generated a prototype that produced three (3) OTPs, correspond to the three (3) Quick Responds codes. Out of the three OTPs generated, it is only one that is meant to be correct while the remaining two OTPs are incorrect. Each of the OTPs generated has a representation of the corresponding password, which is sent to the user as SMS. Similarly, Hammood et al.,[4], carried out research and the transmission medium were through SMS-based medium which is vulnerable to various attack mechanisms. In research carried out by Wang et al., [11], the researchers developed an AUSERA model used to identify the security weaknesses of the global banking applications but the sensitive data of the users were stored using SMS outbox before the actual identification of the weakness.

TABLE 1: The Analysis of the SMS-Based Authentication medium

Author(s) name(s) and Year of Publication	Research Title	Transmission Medium
Ali et al., [2]	Enhanced multi-factor out of bound authentication, En route to securing SMS-based OTP	The verification code generated was transmitted to the user's device through SMS
Ramasamy, Ranganathan, & Palanisamy,[8]	Securing one-time password generation using elliptic curve cryptography with self-portrait photograph for mobile commerce applications.	The OTP generated was sent to the user through SMS to complete the transaction
Hammood et al., [4]	A review of user authentication model for online banking system based on mobile IMEI number.	The OTP transmission was through SMS to the user's device.
Xu et al.[12]	Implicit secondary authentication for sustainable SMS authentication	Transmitted the OTP to the user's device through SMS
Wang et al., [11]	An empirical assessment of security risks of global Android banking apps.	The researchers identified the weaknesses of the banking apps when the sensitive information of the users was stored on the out box of the SMS.
Yin et al., [13]	An efficient two-factor authentication scheme based on the Merkle tree	The OTP generated were sent to the server through the user's device.
Pranata & Nugroho, [7]	2FYSH: Two-factor authentication you should have for password replacement.	The user's device was used to store the private key meant for decryption
Papaspirou et al., [6]	A novel two-factor HoneyToken authentication mechanism	The researchers transmitted the generated OTP the user's device via SMS
Jr. & Vibar, [5]	Authentication key-exchange using SMS for web-based platforms.	The OTP transmission channel was through the user's device
Reese et al.,[9]	A usability study of five two-factor authentication methods.	The secret key was transmitted to the user's device, and the user receives the verification code through the device as SMS.

Table 1 shows that the transmission medium of the generated OTPs from the existing research was through SMS-based authentication processes while the conceptual diagram of the existing transmission medium is depicted on the figure 1. This has clear evidence of the transmission medium of the existing research, where the server generates the OTP and transmits to the user/device, while the user receives the OTP codes and transmits back to the server.

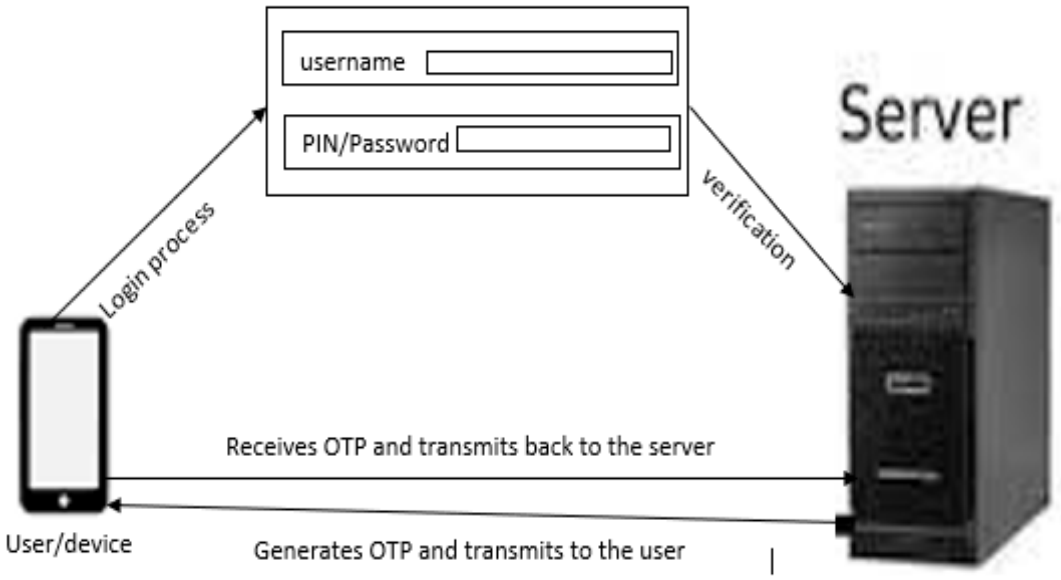

Figure 1: Conceptual Diagram of the Existing Transmission Medium

Table 2: Analysis of the Transmission Medium

Data transmitted	Transmission Medium Analysis
The OTP generated was sent to the user's device through SMS	The user's device could be stolen in order to have access to the generated OTP and possibly use it to complete a transaction. The OTP could be intercepted on transit by various attack mechanism such as MITM, replay, eavesdropping among others The OTP the user received was the same OTP the same user entered into his/her device and transmitted back to the server The OTP delivery time was not determined since it could be delayed as a result of network issues or replay attack An intruder could divert the destination of the OTP to illegitimate destinations
SMS-based transmission medium	SMS-based protocol could be attacked on transit by MITM, replay eavesdropping, grabber, black hat, among others SMS-based protocol is not reliable to store sensitive information because it is used for store and forward, which could replicate messages and forward to various destinations.

3. RESEARCH METHODOLOGY

The SMS-based medium analysis was carried out to identify the transmission medium of the existing research and the specific attack mechanism targeted on each medium for other researchers to gain insights on the attack mechanisms and processes as captured on both tables 1 & 2. Thus, these tables enable the researchers to identify an adequate research method suitable to bridge the attack mechanism of the transmission medium.

However, having seen the transmission medium analysis of the SMS-based medium, it is urgently demanded that the initiating device should be verified to know when an illegitimate device is used to initiate a request. Hence, this leads to the idea of the proposed research developing a model known as the International Mobile Equipment Identity (IMEI) Authentication Technique (IAT) to verify the IMEI number of any initiating device before access is granted to a prospective user.

Thus, every prospective user must register his/her device with the system, where the IMEI number, device type, and device color will be captured at the registration phase. Therefore, on transaction request, the verification of the aforementioned factors will be done to grant access to the device if the verification is successful. Hence, the figure 2 depicts the high-level architecture of this research, which shows a five-level-architecture. This include the registration of the device, the authentication of the user claimed identities, the verification of the device IMEI number through Kerberos authentication and lastly, the actual business layer, which authenticates the actual user's account details to confirm if the user's claim is available or not.

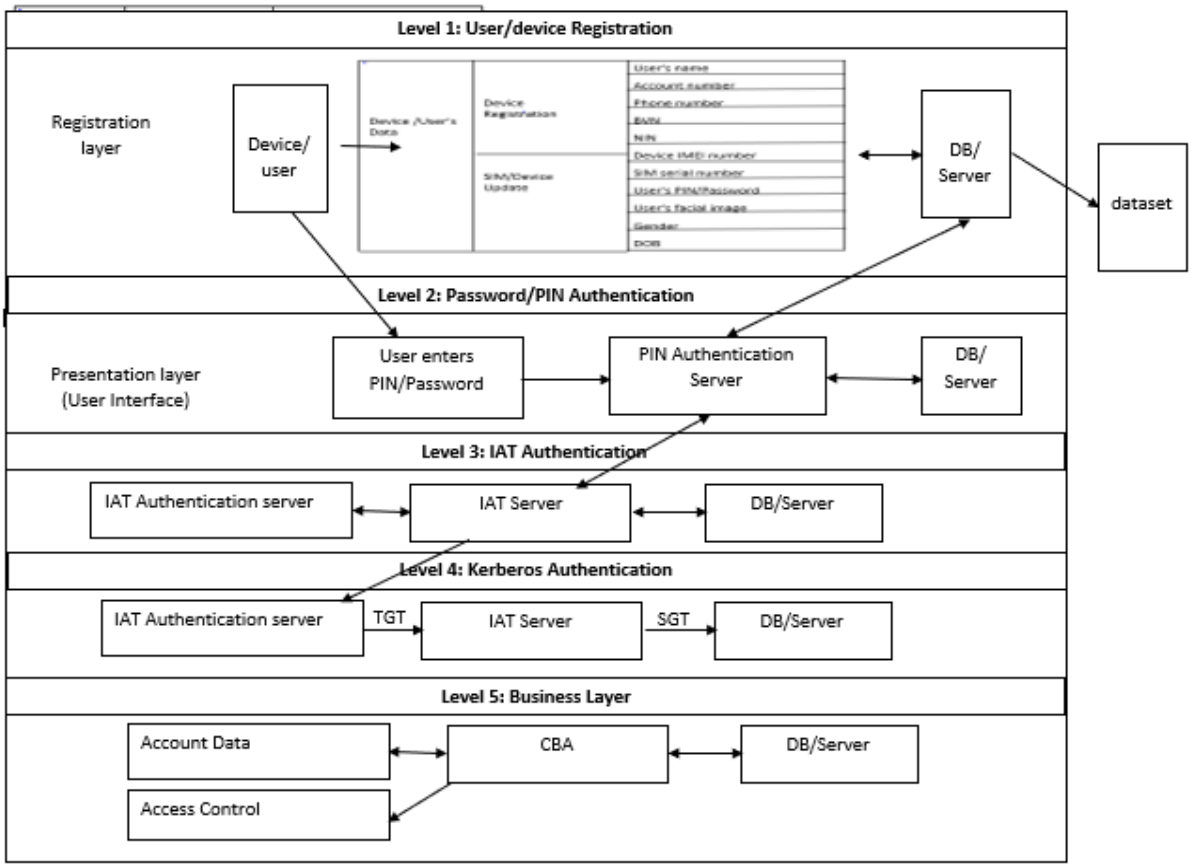

Figure 2: High level architecture of this research

When a request is initiated, through this research model application, the IAT server verifies the IMEI number of the device that initiates such request and communicates with the core banking apps (CBA), if the verification is successful, otherwise, the process will be declined. The diagram on figure 3 illustrates further on this process.

4. RESULTS

Most importantly, the transmission medium of the verification mechanism through the Kerberos transmission medium was adopted in this research among other authentication medium since it is resistant to MITM attack, replay attack among others, as outlined in the analysis of the existing research. Also, it has dual authentication processes, whereby both the server and the user/device is being authenticated for secured communication. The figure 4 depicts the Kerberos transmission medium.

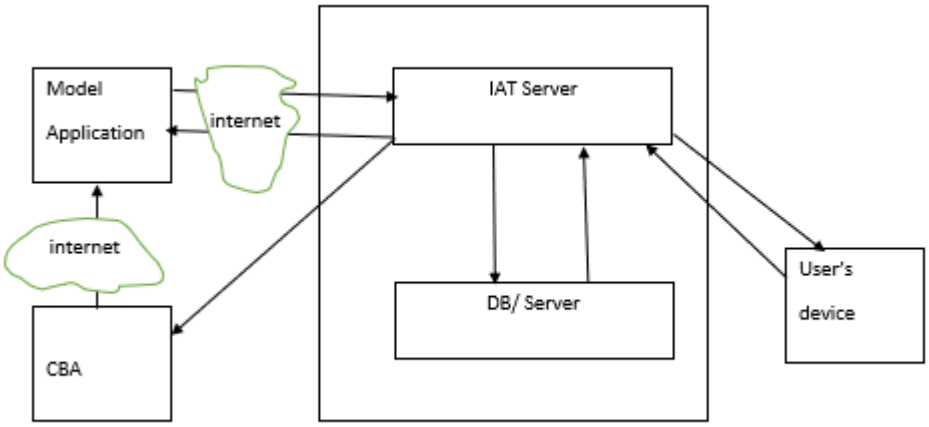

Figure 3: The conceptual framework of this research

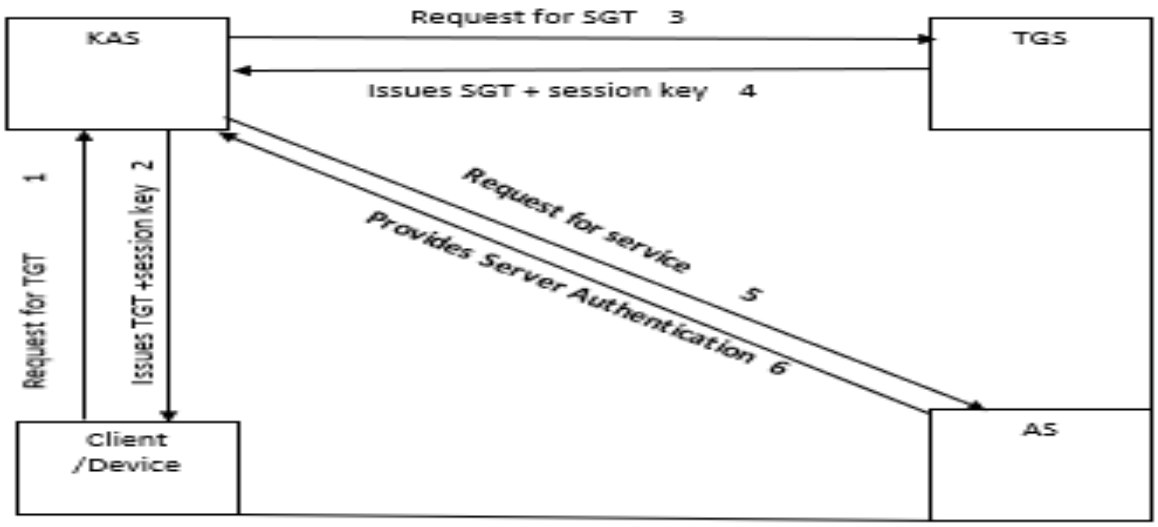

Figure 4: Kerberos transmission medium

Although, the Kerberos authentication medium has six different phases of authentication processes, which starts when an initiator initiates a request to obtain a Ticket Granting Ticket (TGT) from the Kerberos Authentication Server (KAS). When the Kerberos authentication server (KAS) successfully verifies the initiator's claimed identities, it issues Ticket Granting Ticket (TGT) to such initiator, which should be transmitted to the Ticket Granting Server (TGS), requesting for the Service Granting Ticket (SGT) from TGS.

The TGS issues the SGT together with the session key to the initiator. Then, the initiator transmits the SGT obtained from the TGS to the Application Server (AS) requesting for the Service Ticket (ST). Thus, the AS authenticates KAS to confirm if the request is coming from a trusted party, checks the generation time of SGT and expiration time before issuing a ST to the initiator, which is finally transmitted to the core banking applications (CBA) for upward authentication on the account details of the initiator. The mutual authentication mechanism makes the Kerberos authentication medium to have utmost security measure in curbing out the various attack mechanisms such as replay, eavesdropping among others.

However, the Kerberos authentication process used in this research focused on device authentication mechanism. The user only logs into the system with an encrypted secret key that identifies the user's log in details at the backend when decrypted. The actual login details of the user are not transmitted, rather, a shared secret key that identifies the actual login details are being transmitted on transit to be decrypted at the backend.

5. CONCLUSION

The urgent need to tackle the security challenges of SMS-based authentication medium necessitated the importance of this research. The research analyzed the existing transmission medium of the authentication mechanisms and realized that most of the existing research transmitted the sensitive information of the users through SMS-based medium, which is vulnerable to various attack mechanisms. Also, the authentication process was user-based authentication. Hence, this research has deemed it necessary to enhance the authentication medium from user authentication to both user/device authentication and transmission medium using Kerberos authentication method, such that both the initiating device and the user will be authenticated to ascertain the statutory genuineness and secured transmission before access is granted to perform a transaction. However, the researchers recommend further research on server's notification and mitigation on stolen devices to avert fraudulent attack.

References

[1] Kaur, A., , & Mustafa, K. (2019). A Critical appraisal on Password based Authentication. *International Journal of Computer Network and Information Security*, *11*(1), 47–61. https://doi.org/10.5815/ijcnis.2019.01.05

[2] Ali, G., Dida, M. A., & Sam, A. E. (2020). *Two-Factor Authentication Scheme for Mobile Money : A Review of Threat Models and Countermeasures*. 1–28. doi:10.3390/fi12100160

[3] Arif, I., Aslam, W., & Hwang, Y. (2020). Barriers in adoption of internet banking: A structural equation modeling - Neural network approach. *Technology in Society*, *61*(May). https://doi.org/10.1016/j.techsoc.2020.101231

[4] Banga L. and Pillai (2021), Impact of Behavioural Biometrics on Mobile Banking System. Journal of Physics: Conference Series. dio:10.1088/1742-6596/1964/6/062109.

[5] Dadakhanov, S. (2020), Analyze and Development System with Multiple

Biometric Identification.

[6] Hammood, W. A., Abdullah, R., Hammood, O. A., Mohamad Asmara, S., Al-Sharafi, M. A., & Muttaleb Hasan, A. (2020). A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number. *IOP Conference Series: Materials Science and Engineering*, *769*(1). https://doi.org/10.1088/1757-899X/769/1/012061

[7] Jr., B. B. B., & Vibar, J. C. N. (2021). Authentication Key-Exchange Using SMS for Web-Based Platforms. *Journal of Computer and Communications*, *09*(08), 1–12. https://doi.org/10.4236/jcc.2021.9800

[8] Papaspirou, V., Maglaras, L., Ferrag, M. A., Kantzavelou, I., Janicke, H., & Douligeris, C. (2021). A novel Two-Factor HoneyToken Authentication Mechanism. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2021-July*(January 2021). https://doi.org/10.1109/ICCCN52240.2021.9522319

[9] Pranata, S., & Nugroho, H. T. (2019). 2FYSH: Two-factor authentication you should have for password replacement. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(2), 693–702. https://doi.org/10.12928/TELKOMNIKA.V17I2.9187

[10] Ramasamy, P., Ranganathan, V., Palanisamy, V., & Kadry, S. (2020). Securing one-time password generation using elliptic-curve cryptography with self-portrait photograph for mobile commerce application. *Multimedia Tools and Applications*, *79*(23–24), 17081–17099. https://doi.org/10.1007/s11042-019-7615-3

[11] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., Seamons, K., Clara, S., Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). *A Usability Study of Five Two-Factor Authentication Methods This paper is included in the Proceedings of the*. 357–370.

[12] Ryu, G., & Kim, S. (2019). *Implicit Secondary Authentication for Sustainable SMS Authentication*. 1–15. https://doi.org/10.3390/su11010279

[13] Wang, D., Zhang, X., Wang, C., Niu, W., Ming, J., & Chen, T. (2018). *Resetting Your Password Is Vulnerable : A Security Study of Common SMS-Based Authentication in IoT Device*. *2018*. https://doi.org/10.1155/2018/7849065

[14] Xu, G., Qiu, S., Ahmad, H., Xu, G., Guo, Y., Zhang, M., & Xu, H. (2018). A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography. *Sensors (Switzerland)*, *18*(7), 1–19. https://doi.org/10.3390/s18072394

[15] Yin, X., He, J., Guo, Y., Han, D., Li, K. C., & Castiglione, A. (2020). An efficient two-factor authentication scheme based on the Merkle tree. *Sensors (Switzerland)*, *20*(20), 1–19. https://doi.org/10.3390/s20205735