Assignment Report

Multi-factor Authentication

Student Name:

Student Id:

Year: 2024

Words: 2571

1. Executive Summary

This project derives about various type of multi-factor authentication methods like passwords, fingerprints, Face Ids, OTP codes and hardware tokens. Each of these security methods are in detail in terms of technical complexity, user access, and legal compliance. Passwords are not safer method anymore because of it's easily can be hacked. When you locked in biometrically, you're stuck. If you think OTP is safer method it can be a part of a big issue, when you're using another SIM card. The project explicit the minor usage of tailor-made MFA systems while increasing the challenge of the security consideration for banking sector and public services. This research gives the suggestions for adoptive MFA solutions and the authentication that have high risk to improve the level of security and functionality. These studies conducted on machine leaning in adaptive MFA, decentralized identity creation and modifications to the legal system to make MFA more useful in real-world situations, technical complexity, user access and legal compliance.

Table of Content

2. Background of the Issues

2.1 Topic being studied

2.1.1 Importance of Topics

Multi-Factor authentication is most important topic in banking, government and e-commerce sectors. There are advantages and disadvantages of that all authentication methods. Biometrics may not be as perfect with injuries, while increase convenience. And the passwords can be hacked anytime with the usability. So, MFA is playing significant roll to prevent unauthorized accesses, but on the other hand, there may have been impediments such as regulatory measures, accessibility and compatibility procedures for account resets and identification.

Group Member	Learning Outcome	Responsibilities
Member 1	Express analytical skills and develop critical thinking in MFA methods.	Research about biometric authentication and it's challenges.
Member 2	Improve the understanding of cyber security regulations in MFA with related compliance issues.	Analyze the regulatory body with MFA implementations.
Member 3	Enhance skills of problem solving by using technical limitations and suggesting other solutions.	Explore recovery methods and non-technical factors for accounts.
Member 4	learned about user experience and usability issues with the introduction of MFA. Enhance collaborative skills in research and synthesis findings.	Investigate about accessibility issues along with passwords, SMS codes and hardware tokens. Conduct discussions, compile information and draft the final report on MFA adoption issues.
Member 5	strengthened teamwork abilities in organizing research and synthesizing results.	Organize group discussions, compile data, and draft the final report on the adoption of MFA and its difficulties.

Table 1: 2.2 Tables of learning outcomes responsibilities of individual team members

2.2.1 Focus the team collectively

Along with the other elements, team should consider technical side of MFA. Team test about security, accessibility, legacy rules and procedures as well as pros and cons of most of MFA methods such as biometrics, SMS codes, TOTP codes, hardware tokens, and passwords (Amft et al. 2023).

2.3 Relevant Literature Review

2.3.1 Annotated review of key item(s) for each part of the project

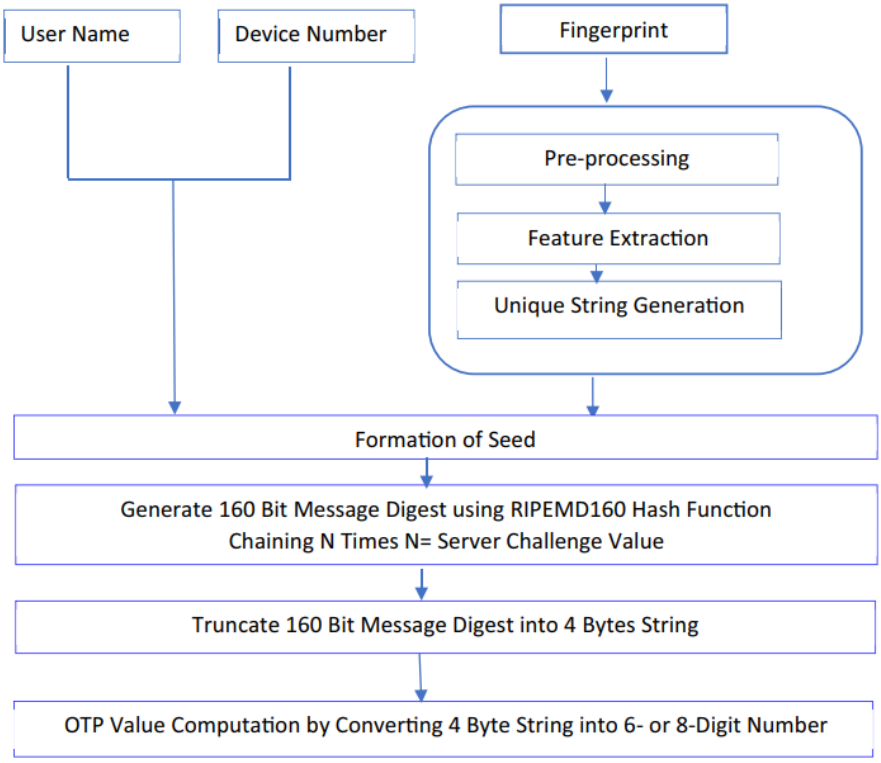

Figure 1 : Proposed OTP generation process

Source: Lone & Mir (2022)

Passwords:

Passwords can be guesses easily, socially engineered or contain malicious insiders and user tend to use very weak passwords. Then that became an isecure authentication method in modern times according to Hassen et al. (2004). But this authentication method available on most of the applications. Passwords are still use often. However, It's not an safer and reliable way in modern form of security.

Biometrics:

According to In the words of Kirfel et al. (2022) Biometrics are in several forms in modern world like face recognition, fingerprint and voice recognition. But there are some issues such as Fingerprints can be removed by staining or erasing the skin, and once obtained, these biometric details can be destroyed. If that destroyed biometric cannot retrieve like other authentication methods.

SMS and TOTP Codes:

OTP is the second popular factor across the authentication methodologies, but it also not safer method either. Although TOTP is more secure than traditional time-based passwords (Lone & Mir, 2022).

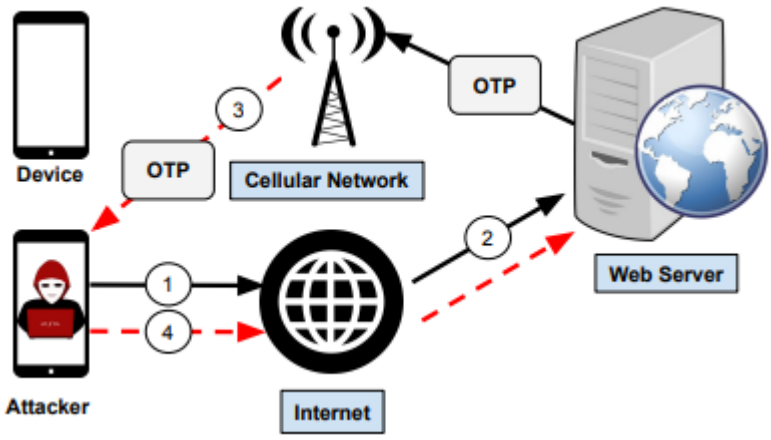

Figure 2 : In a SIM Swap attack, an adversary obtains a replacement SIM card for a target user through a cellular network provider.

Source: Peeters et al. (2022)

Hardware Tokens and Passkeys:

YubiKeys are one of the physical tokens that supports public-key cryptography, authentication, and the Universal 2nd Factor. Passkeys are new authentication method and it more user-friendly. Nevertheless, their low acceptance rates can be attributed to their incompatibility with multiple platforms.

.

2.3.2 Summary of Related Literature

The multi-factor authentication has several MFA methods. Research targets to improve security interventions that addressing complex barriers related to accessibilities and rules.

3. Issues

3.1 Problems analysed

3.1.2 Definitions of problems

The main challenge of MFA is different approaches to implementing MFA and the problems commonly the issues that are frequently connected to them. Signs and passwords ease to hack from careless users (Shukla et al. 2024).

Authentication methods such as biometric safer than traditional authentication methods like passwords. But as a example it affected to finger configuration if there was physical damage or finger injuries. So, biometrics not suited anytime and anywhere (Dragon & Kumar, 2020).

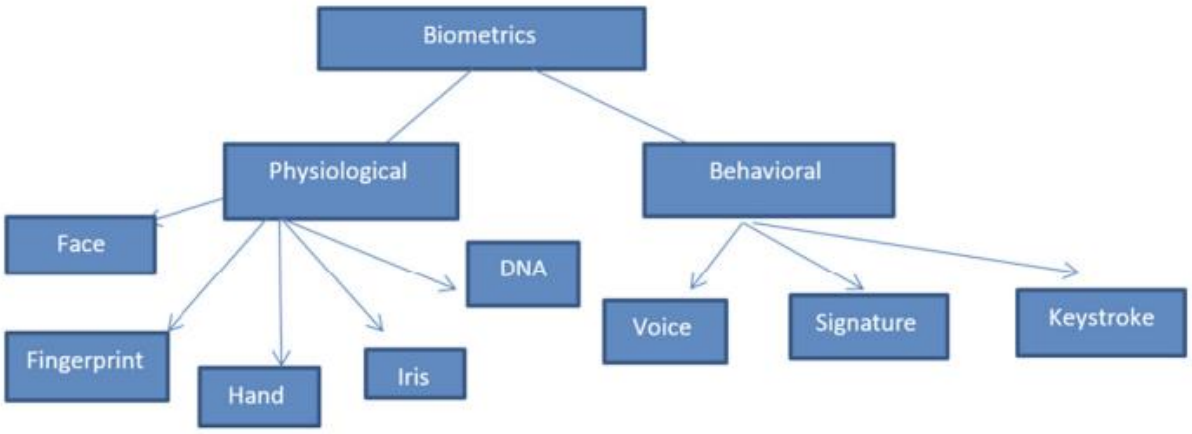

Figure 3 : Classification of physiological and behavioural biometrics

Source: Abdulrahman & Alhayani (2023)

SMS based TOTP also has some obstacles. Traceability of the sim data and swapping SIM cards rapidly may be harmful for our security. TOTP still secures than the other authentication methods. But they are not convenient for an all users, especially clients with less technical skills affect user acceptance and satisfaction (Peeter et al. 2022). Cryptographic tokens safer option relatively other authentication methods. But the cost is high as well as the security.

Evolving Technology always hind for regulations in implementing MFA. And the other hand, the northern government's act of ID verification is the second step in account recovery processes and verification highlights the need of creativity, user-friendly approaches and server as a roadblock to the further development of such complex techniques.

3.2 Importance of problems

3.2.1 Why are problems as important as IT problems?

Passwords became a huge vulnerability in modern cyber security cause it can being a victimized of advanced form of cyber-attacks (Wee, Checkol, & Shaw, 2024).

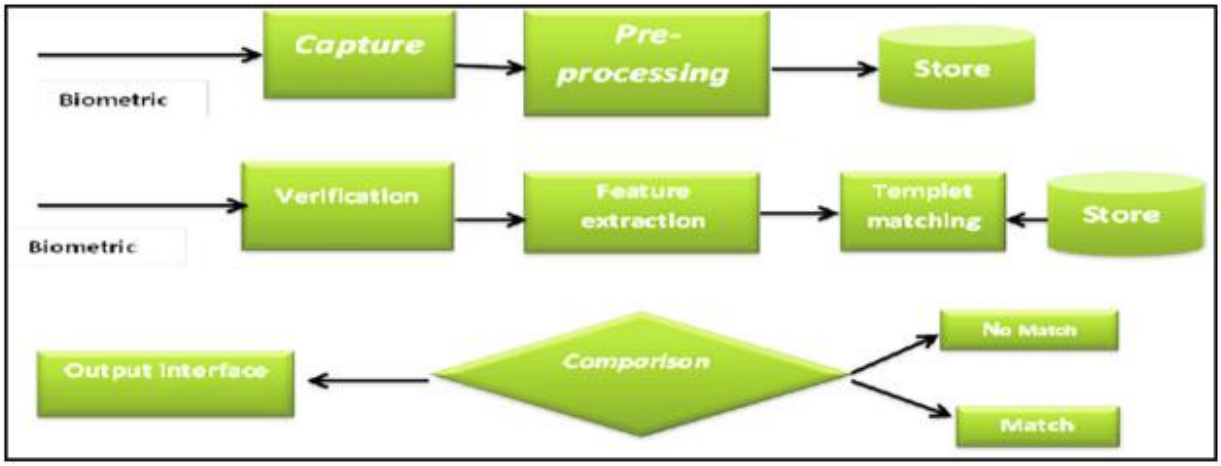

Figure 4 : Stages of authentication/registration process using biometrics

Source: Abdulrahman & Alhayani (2023)

Biometric authentication depends on physiological characteristics. That was a unique IT problem in that authentication method. Biometric data cannot be hacked or trace. But if it penetrate once it poses a huge security threat (Abdulrahman & Alhayani, 2023). There is a difference between hardware and software biometric systems, and it always lead failure in authentication process cause of user influence.

Group Member	Marks Criteria	Responsibilities
Member 1	Research Depth and Critical Analysis (25%)	Conduct in-depth research on MFA methods and critically analyse biometric and password-based authentication.
Member 2	Regulatory and Compliance Analysis (20%)	Examine cybersecurity regulations and analyse how they impact MFA adoption, particularly in the banking and government sectors.
Member 3	Problem-Solving and Solution Development (20%)	Identify technical and usability challenges in SMS, TOTP codes, and hardware tokens, proposing viable solutions.
Member 4	User Experience and Accessibility Evaluation (15%)	Investigate and evaluate the accessibility and user experience of MFA methods, focusing on inclusivity and ease of use.
Member 5	Group Coordination and Presentation (20%)	Oversee group coordination, ensure timely completion of tasks, and compile findings into a cohesive report and presentation.

Table 2 : 3.3 Table of Scoring Criteria Responsibilities of Team Members

4. Analysis of Issues

4.1 Detailed analysis of the identified issues

4.1.1 Different interpretations of problems

Multi-factor authentication (MFA) is characterized by many interpretations based on the stated challenges, including technical, usability and regulatory concerns. Szpunar & Stęchły (2023) claim that password-dependent MFA is insecure because, despite their widespread use, passwords are inherently weak due to poor password hygiene provided by users. Although biometric authentication is thought to be secure, there are some difficulties due to changes in physical characteristics or damage to fingers, eyes or even face.

The problem with permanently backing up data is the latter. SMS-based techniques are prone to SIM switching incidents, and TOTP code input can be challenging, especially for older people. However, passkeys, modern hardware tokens, and similar tokens, despite their relative security, are neither ergonomic nor inexpensive (Lee, Kaiser, Mayer, & Narayanan, 2020).

4.2 Disciplinary knowledge and skills used from other units

4.2.1 Contribution of various chiefs

Multi-factor authentication (MFA) testing involves knowledge and skills spread across several disciplines. Applying cybersecurity principles can analyze problems with contemporary authentication methods, including threats such as SIM swapping and data breaches (Solove & Hartzog, 2022). The logic of legal and compliance studies contributes to the analysis of archetypal regulations that impede the implementation of MFA. Both UX and design aspects are important knowledge to assess accessibility issues and ensure that advanced MFA solutions are accessible and easy to use for all types of users and their disabilities. IT recommends technical evaluation of hardware tokens, TOTP codes, as well as passkeys (Amft et al., 2023). Overall, these interdisciplinary approaches contribute to the study and offer sustainable solutions that are applicable to various fields such as banking or government.

Strategy	Anticipated Costs	Expected Benefits
Implementation of Backup Solutions	Hardware, software, and backup setup costs	Increased data protection, reduced unauthorised access
Upgrading Authentication Technologies	Audit fees, documentation, and legal costs	Improved user compliance, reduced security risks
Regulatory Compliance Audits	Equipment costs, maintenance, and updates	Enhanced system reliability, improved user experience
User Training and Awareness Programs	Training materials, implementation costs	Improved user compliance, reduced security risks
Enhanced MFA Security Protocols	Software development, integration costs	Increased data protection, reduced unauthorised access

Table 3 : 4.3 Projected profit and loss table

There are some advantages in multi-factor authentication,

- Reduce the cost of software development and end user training
- Improve data protection
- Increased end-user compliance
- Increased system reliability

Long-term security breach perspectives (Long-term security breach perspectives). These strategies mitigating the threats from hackers, viruses, etc. and it is a fundamental requirement for efficiently secure such information and decrease system breakdowns, time losses and unauthorized accesses, moreover, it improves operational safety in cost-effective situations (Perwej et al., 2021).

Category	Assets	Liabilities	Equity
Current Assets			
Cash	$50,000		
Accounts Receivable	$20,000		
Total Current Assets	**$70,000**		
Non-Current Assets			
Technology Investment	$30,000 (MFA software and equipment)		
Training Programs	$10,000 (User training costs)		
Total Non-Current Assets	$40,000		
Total Assets	**$110,000**		
Non-Current Assets			
Technology Investment	$30,000 (MFA software and equipment)		
Training Programs	$10,000 (User training costs)		
Total Non-Current Assets	$40,000		
Total Assets	**$110,000**		
Current Liabilities			
Accounts Payable		$15,000	
Short-Term Debt		$10,000	
Total Current Liabilities		**$25,000**	
Long-Term Liabilities			
Loan for Tech Upgrade		$20,000	
Total Long-Term Liabilities		$20,000	
Total Liabilities		**$45,000**	

Equity			
Retained Earnings			$65,000
Total Equity			$65,000
Total Liabilities and Equity		**$110,000**	

Table 4 : 4.4 Projected balance sheet

Above table shows liabilities that associated technology investments with various MFA stategies. Then it’s show enhancement of the security using retained earnings.

5. Conclusion

5.1 Summary of key points from the study

This report expresses the pros and cons of multi-factor authentication in banking, public services and e-commerce sectors. Some of that issues and risks associated with commonly passwords, feasibility of using biometrics, effective use of TOTP and hardware tokens. MFA also has such hinds as Legal requirements, accessibility concerns, and challenges with account recovery. Overall study discuss that context-sensitive, easy-to-use MFA solutions are essential to improve security, compliance and the best user experience.

5.2 Recommended solutions

We recommend adaptive MFA systems that select the most appropriate solution in user device, location and his/her behaviour. It became now as password less technologies like passkeys to ensure security strength ability. By referring risk value of each access attempt, we can estimate the security level of risk-based authentication methods. However, disable people also can avoid issues of the other authentication methods like biometric using this MFA. MFA will become more practical and applicable to a wider range of businesses and sectors.

5.3 Suggestions for further research or development

AI algorithms are access the activities that human interacted which study done that part of study about adaptive MFA approach. Decentralized Id systems nowadays much popular with a blockchain to secure data management. Current restrictions will be lifted in part by the effect of regulatory changes on MFA acquisition and the development of best practice guidelines to offer simple, widely secure authentication solutions.

6. Future Plans

6.1 Planned careers or future study - (each group member individually)

Each group member individually	Future Plans
Member 1: Cybersecurity Analyst	Aspires to pursue a career in cybersecurity, focusing on research and analysis of authentication methods and security technologies. Plans to undertake further studies in cybersecurity with a specialisation in identity and access management.
Member 2: Compliance Officer in Financial Technology	Aims to work in regulatory compliance within the financial technology sector, focusing on how regulations impact security technologies. Intends to pursue certifications in cybersecurity law and compliance.
Member 3: IT Solutions Architect	Plans to become an IT solutions architect, specialising in designing secure authentication systems. Interested in further studies in systems engineering and advanced cybersecurity frameworks.
Member 4: UX Designer in Security Technology	Aspires to work as a UX designer specialising in security applications, ensuring accessible and user-friendly security solutions. Plans to further study human-computer interaction and inclusive design principles.
Member 5: Project Manager in Tech Development	Intends to pursue a career in project management within technology development, focusing on coordinating security projects. Plans to enhance skills through certifications in project management and leadership in tech environments.

Table 5 : Future plans for each group members

6.2 Reflection on group research: strengths and weaknesses

This section about strength of multi-factor authentication with our research observations. Each and every member has unique skill set and knowledge about the topic. It was a great experience for us to conduct this research. Healthy communication and close cooperation made the integration among team members. Then it is the result of this complete and on-time report, as we expected. According to critical analysis, We used this ability to analyse the benefits and drawbacks of every verification technique while presenting accurate data.

On the other hand, we can recognize some weaknesses in our workflow. There are time management issues, delays in integrating research findings, Poor exposure to the most recent and up-to-date literature on some of the new MFA technologies now under development limits the study. We should pay our attention more about time management and up to date sources, and the work can get as an organized collaboration work of my team, and it finalize as a result of successful workflow.

References

Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80, 2642-2646. https://doi.org/10.1016/j.matpr.2021.07.005

Ali, G., Dida, M. A., & Elikana Sam, A. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. https://doi.org/10.3390/fi13120299

Amft, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023). Lost and not Found: An Investigation of Recovery Methods for Multi-Factor Authentication. https://publications.cispa.de/articles/journal_contribution/Lost_and_not_Found_An_Investigation_of_Recovery_Methods_for_Multi-Factor_Authentication_/25186640

Amft, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023, November). " We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 3138-3152). https://doi.org/10.1145/3576915.3623180

Angelogianni, A., Politis, I., & Xenakis, C. (2024). How many FIDO protocols are needed? Analysing the technology, security and compliance. ACM Computing Surveys, 56(8), 1-51. Retrieved 06 September 2024 from: https://doi.org/10.1145/3654661

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, 113114. https://doi.org/10.1016/j.eswa.2019.113114

Hasan, M., Rozony, F. Z., Kamruzzaman, M., & Uddin, M. K. S. (2024). COMMON CYBERSECURITY VULNERABILITIES: SOFTWARE BUGS, WEAK PASSWORDS, MISCONFIGURATIONS, SOCIAL ENGINEERING. Global

Mainstream Journal of Innovation, Engineering & Emerging Technology, 3(04), 42-57. https://doi.org/10.62304/jieet.v3i04.193

Jacomme, C., & Kremer, S. (2021). An extensive formal analysis of multi-factor authentication protocols. *ACM Transactions on Privacy and Security (TOPS)*, *24*(2), 1-34. https://doi.org/10.1145/3440712

Kirfel, A., Scheer, T., Jung, N., & Busch, C. (2022). Robust identification and segmentation of the outer skin layers in volumetric fingerprint data. Sensors, 22(21), 8229. Retrieved 06 September 2024 from: https://doi.org/10.3390/s22218229

Lee, K., Kaiser, B., Mayer, J., & Narayanan, A. (2020). An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth symposium on usable privacy and security (soups 2020)* (pp. 61-79). https://www.usenix.org/conference/soups2020/presentation/lee

Lone, S. A., & Mir, A. H. (2022). A novel OTP based tripartite authentication scheme. International Journal of Pervasive Computing and Communications, 18(4), 437-459. https://doi.org/10.1108/IJPCC-04-2021-0097

Peeters, C., Patton, C., Munyaka, I. N., Olszewski, D., Shrimpton, T., & Traynor, P. (2022, May). SMS OTP security (SOS) hardening SMS-based two factor authentication. In Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security (pp. 2-16). https://doi.org/10.1145/3488932.3497756

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710. https://dx.doi.org/10.18535/ijsrm/v9i12.ec04

Shukla, S., Varshney, G., Singh, S., & Goel, S. (2024). A Passwordless MFA Utlizing Biometrics, Proximity and Contactless Communication. arXiv preprint arXiv:2406.09000. https://doi.org/10.48550/arXiv.2406.09000

Solove, D. J., & Hartzog, W. (2022). *Breached!: Why data security law fails and how to improve it*. Oxford University Press. https://books.google.com/books?hl=en&lr=&id=yvJbEAAAQBAJ&oi=fnd&pg=PP1&dq=Applying+cybersecurity+principles+++SIM-swapping+data+breaches&ots=sPZsBBmPln&sig=nO3avEkNT7UH_8HrHtwOAhjrWRA

Szpunar, A., & Stęchły, A. (2023). Analysis of potential risks of SMS-based authentication. *Advances in Web Development Journal*, *1*, 13-25. https://bibliotekanauki.pl/articles/31233158.pdf

Wee, A. K., Chekole, E. G., & Zhou, J. (2024). Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis. arXiv preprint arXiv:2407.20459.https://doi.org/10.48550/arXiv.2407.20459