Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems

by Asyura Binti Sofian

Submission date: 18-Jul-2024 10:12AM (UTC+0700)
Submission ID: 2418508322
File name: 527-IJCTS_Asyura_Binti_Sofian_74207_TME4433_GroupProject.pdf (480.82K)
Word count: 5124
Character count: 32938

International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 56-70
DOI: https://doi.org/10.62951/ijcts.v1i3.24
Available online at: https://international.arteii.or.id/index.php/IJCTS

Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems

Asyura Binti Sofian[1], Ayu Fitri Alafiah Binti Peradus[1], Fidel Yong[1], Irvine Shearer Anak Junit[1], Nurrul Nazwa Binti Ismail[1], Yugendran A/L Mahendran[1] & Muhammad Faisal[2]

[1] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kuching, Sarawak, Malaysia;*
[2]*Director HRIMS, Ministry of Human Rights*

74207@siswa.unimas.my 74232@siswa.unimas.my 73460@siswa.unimas.my 75062@siswa.unimas.my 76391@siswa.unimas.my 73882@siswa.unimas.my dr.faisalshabbir88@gmail.com

Abstract— *This paper explores the Time-Based One-Time Password (TOTP) authentication mechanism enhanced with lightweight cryptographic algorithms, presenting it as an advanced solution to the limitationsof traditional OTP systems. There are a lot of applications and systems where this mechanism is applied. For example, bank applications, e-commerce websites, access control system, healthcare system, etc. TOTPgenerates dynamic, time-sensitive passwords using the current time and a secret key processed through a cryptographic hash function, significantly improving security by reducing vulnerabilities to code reused and interception. The adoption of lightweight algorithms ensures that TOTP can be efficiently implementedon resource-constrained devices, such as those on the Internet of Things (IoT) ecosystem. Despite its benefits, TOTP faces challenges including synchronization issues between client devices and servers, and a trade-off between computational efficiency and security strength. This paper discusses the implications of these challenges and evaluates how TOTP, with appropriate design considerations, can provide a robust,secure, and efficient authentication method suitable for various applications, from digital banking to IoT environments.*

Index Terms— *OTP, TOTP, Lightweight Algorithm*

1. INTRODUCTION

Time-Based OTP (TOTP) is an improved version of the traditional One-Time Password (OTP) system, enhanced with lightweight algorithms. Unlike traditional OTP systems that use a running counter, TOTP creates a one-time password based on the current time and a secret key, processed through a cryptographichash function [1]. This makes the OTP change every 30 seconds, adding a dynamic layer of security that lowers the risk of code reuse and interception. A key feature of TOTP is the use of lightweight cryptographicalgorithms. These algorithms are designed to reduce computational load, making TOTP ideal for Internet of Things (IoT) devices, which often have limited processing power, memory, and battery life. By using lightweight algorithms, TOTP can maintain high security standards without exhausting the resources of these constrained devices. However, there are challenges in implementing this method. One of the issues issynchronization between the client device and the authentication server. Additionally, there is a trade-off between security and computational efficiency, and the vulnerability of OTP to brute force attacks remainsa concern.

The evolution of authentication mechanisms is driven by the increasing complexity and interconnectivity of modern digital ecosystems. With the proliferation of IoT devices, the need

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 15, 2024; Published: July 18, 2024;
* Asyura Binti Sofian , 74207@siswa.unimas.my

for robust, efficient, and scalable authentication methods has become more critical than ever. Traditional authentication mechanisms, such as static passwords, have proven inadequate in protecting against sophisticated cyber threats. As these threats evolve, so must the methods to counteract them. TOTP, with its time-based approach, offers a promising solution that addresses many of the limitations of older systems. Its adaptability to various environments, from digital banking to industrial IoT, showcases its versatility. Furthermore, the integration of lightweight cryptographic algorithms ensures that even devices with minimal processing capabilities can implement TOTP effectively. This balance between security and efficiency makes TOTP a viable candidate for widespread adoption in diverse application domains, ensuring secure and seamless user experiences across platforms.

In summary, TOTP with lightweight algorithms offers a promising solution for secure and efficient two- factor authentication (2FA) in various environments, including IoT, digital banking, and virtual reality. While it solves several issues of traditional OTP systems, careful consideration is needed to handle the limitations and challenges of lightweight cryptographic algorithms to achieve a balanced approach to security and performance. The ongoing evolution of digital threats necessitates continuous improvement in authentication mechanisms, and TOTP's dynamic, time-sensitive approach provides a robust foundation forenhancing security across multiple applications. By addressing synchronization issues and optimizing the trade-offs between security and computational efficiency, TOTP can significantly improve the security landscape for modern digital ecosystems.

Moreover, the integration of TOTP with lightweight algorithms represents a strategic advancement in the realm of cybersecurity. The lightweight nature of these algorithms ensures that TOTP can be deployed on a wide range of devices, from high-end servers to low-power IoT devices, without compromising on performance or security. This adaptability is crucial in today's interconnected world, where diverse devices must communicate securely and efficiently. Additionally, the use of time-based algorithms minimizes the risk of replay attacks, a common vulnerability in static password systems. This temporal component meansthat even if an OTP is intercepted, it becomes useless after a short period, thereby significantly enhancing security.

Furthermore, the implementation of TOTP in critical sectors such as healthcare, finance, and industrial automation can provide robust security measures that protect sensitive data and systems from unauthorizedaccess. In healthcare, for instance, TOTP can secure patient records and ensure that only authorized personnel can access critical medical information. In the financial sector, it can safeguard online transactions and protect against fraud. In industrial

automation, TOTP can secure control systems and prevent unauthorized access to critical infrastructure. The versatility and robustness of TOTP with lightweight algorithms make it an essential tool in the modern cybersecurity toolkit, capable of addressing the diverse and evolving threats in various sectors.

2. RELATED WORKS

2.1. TOTPAuth: A Time-based One-Time Password Authentication Proof-of-Concept againstMetaverse User Identity Theft [2]

In virtual reality (VR) contexts, authentication is essential to guaranteeing safe access to digital resources.In immersive virtual reality environments, conventional techniques such as PIN-based authentication are vulnerable to theft and surveillance. To authenticate users, the suggested method, TOTPAuth, combines a time-based one-time password that is produced by the system with a username and password submission procedure. Security and resistance to surveillance are improved by this technique. In contrast to conventional PIN-based approaches, it does come with a trade-off of somewhat poorer entry accuracy anda longer entry time. Subsequent investigations may concentrate on enhancing entry time and precision while upholding elevated security protocols.

2.2. Bank Application: One-Time Password Generation [3]

Securing online transactions in digital banking requires strong authentication techniques, such as one- time passwords (OTPs). However, malware and phishing assaults can target conventional OTP systems. With the use of encryption techniques like AES and DES, the suggested method provides a secure OTP generating mechanism for financial applications. Enhanced security via dynamic OTP creation and user- friendly authentication are strengths; nevertheless, reliance on mobile devices for OTP transmission and implementation complexity are drawbacks. Future research should examine different OTP distribution strategies to lessen reliance on mobile devices.

2.3. A Blockchain-Based OTP-Authentication Scheme for Constrained IoT Devices Using MQTT [4]

To improve security in IoT devices, the study suggests an OTP authentication mechanism for MQTT thatis based on blockchain. By establishing a distinct authentication channel with Ethereum, it enhances user security and privacy. By utilizing smart contracts and blockchain technology, this approach improves security by mitigating issues with impersonation attacks and single points of failure that are present in the conventional OTP-based system. Nevertheless, it could make implementation more difficult. Subsequent investigations may

concentrate on streamlining the implementation procedure while preserving security standards.

2.4. **Human-Computable OTP Generator as an Alternative to Two-Factor Authentication** [5]

The study highlights the necessity for safe and approachable techniques by going over several authentication strategies and protocols. The Learning with Options (LWO) technique is used in the proposed iChip protocol to increase entropy, while a human-generated OTP protocol is used for secure authentication. Improved defense against assaults is one of the strengths; complexity and usability issues are the drawbacks. Subsequent research attempts may concentrate on enhancing user experience while maintaining security.

2.5. **Performance Evaluation of a New One-Time Password Scheme Using Stochastic Petri Net** [6]

In order to generate a new OTP for authentication, this study suggests a novel OTP system that combinesa user-performed mathematical computation. This technique increases security without adding to the load on server-side verification. Strengths include increased system performance and security, while negatives include possible user operation complexity. Subsequent research endeavours may focus on streamlining mathematical computations to enhance user experience.

2.6. **One-Time Password Authentication for Machine Activation Monitoring System Based on WirelessNetwork**[7]

The difficulties of incorporating current equipment into networked systems and the dangers of mistakesand inefficiency in manual data collection are discussed in this study. An OTP-based authentication technique used in a web-based monitoring system is the suggested remedy. Although it depends on wirelessconnections, which can provide risks, this method provides a lightweight solution with little modification to currently installed equipment. Potential avenues for further study include enhancing wireless connectionsecurity.

2.7. **Providing Security to Land Records with the Computation of Iris, Blockchain, and One Time Password** [8]

In order to safeguard property records, this study proposes a security system that combines blockchain technology, iris recognition, and OTP. By utilizing blockchain transparency and multi-factor authentication, the integrated method lowers the possibility of fraud while providing increased security. Notwithstanding, the intricacy of executing such system and the requirement for substantial modifications to the infrastructure provide obstacles. Subsequent investigations may concentrate on streamlining the execution procedure and diminishing the necessities for infrastructure.

2.8. App-based Detection of Vulnerable Implementations of OTP SMS APIs in the Banking Sector [9]

This paper examines the security of OTP SMS APIs, emphasizing the dangers associated with shoddy implementations, as they are utilized in Spain's banking industry. Through an analysis of the ways in whichvarious banking apps manage OTP SMS, the study pinpoints particular flaws that can enable hackers tointercept or abuse these OTPs. Static and dynamic analysis approaches are used in the suggested method to evaluate these implementations' security. Replicability and methodological rigor are strengths; reliance on API access is a downside. Future research could broaden the investigation to include additional industries and enhance API security generally.

2.9. A Microservices and Blockchain Based One-Time Password (MBB-OTP) Protocol for Security- Enhanced Authentication [10]

This study suggests the MBB-OTP protocol, which decentralizes the processes of OTP creation and dissemination by fusing blockchain technology with microservices design. This approach combines blockchain technology with microservices to improve scalability and security. The ability to withstand DoS and MITM assaults is a strength; implementation complexity is a downside. Subsequent investigations maystreamline the procedure and enhance its scalability.

2.10. Secure One-Time Password Generation Using Shamir's Secret Sharing [11]

This article presents a novel method of combining Shamir's Secret Sharing with Visual Cryptography Schema (VCS) to improve the security of OTP systems. The process divides the OTP into multiple shares,which have little value unless they are merged. This method greatly lowers the chance of unwanted access,but it also makes the system more difficult to maintain and more complex for the end user. Subsequent investigations may concentrate on simplifying the experience for users while upholding elevated security protocols.

2.11. GRAIN Algorithm Implementation for Lightweight Hardware-based OTP Authentication [12]

This paper suggests utilizing the GRAIN encryption method for hardware-based OTP authentication in order to prevent data breaches, considering the problems with traditional OTP systems. This technology offers a lightweight, safe, and quick encryption solution. Improved system performance and increased security are among the strengths; implementation complexity is one of the disadvantages. Subsequent investigations may focus on streamlining the execution procedure while upholding security.

2.12. **A Cutting-Edge Security Solution: OTP-Based Smart Wireless Locking System [**13]

This study's main goal is to analyse the drawbacks of traditional locking systems and provide an improvedOTP authentication lock that runs on an Arduino board. By providing keyless entry and enhanced security, this intelligent wireless locking system lowers the possibility of unwanted access. A user-friendly and secure approach is one of its strengths; on the other hand, its dependence on expensive mobile devices andcertain software capabilities is one of its shortcomings. Future studies can concentrate on lessening the dependence on hardware specifications.

2.13. **Comparative Analysis**

The reviewed studies propose various authentication mechanisms, each with its own strengths and weaknesses. Common themes include the use of blockchain technology for enhanced security and decentralization, multi-factor authentication to improve resilience against attacks, and human-computable methods to increase user-friendliness. While these approaches offer significant improvements over traditional methods, they also introduce new challenges such as complexity in implementation and useroperations.

Several other researchers have also contributed in end-to-end security mechanism even with the assistance of the counter partners i.e. universities or industries for broaden implications [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27]. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work One-Time Password (OTP) for the given problem statement is adopted from [1],which acts as a benchmark for this research article.

3. PROPOSED SOLUTIONS

The more sophisticated approach known as Time-Based OTP (TOTP) with Lightweight Algorithms functions as an improved variant of the One-Time Password (OTP). Instead of using a running counter as its second input, the Time-based One-time Password algorithm (TOTP) uses the current time to generate aone-time password (OTP). A cryptographic hash function that produces an OTP is fed a secret key and the current time as input. Using lightweight cryptographic techniques to lessen the computing burden on Internet of Things devices is crucial.

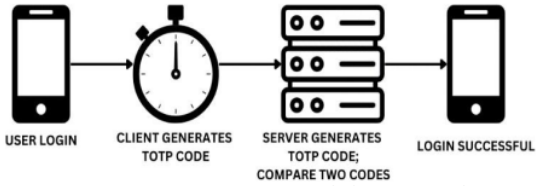

Figure 1: How TOTP validation works

A computer technique that creates a one-time password (OTP) by using the current time as a source of uniqueness is a type of two-factor authentication (2FA). Differentiations between the time the user generates the OTP and the time the server independently generates its OTP might lead to synchronization problems because TOTP employs clock time as one of its inputs into the OTP generating algorithm. As a result, to verify a TOTP, the server needs to analyse a variety of TOTPs produced within a specific window of clock periods (such as 30 seconds). An authenticated user is one who discovers a match withinthis range of TOTPs

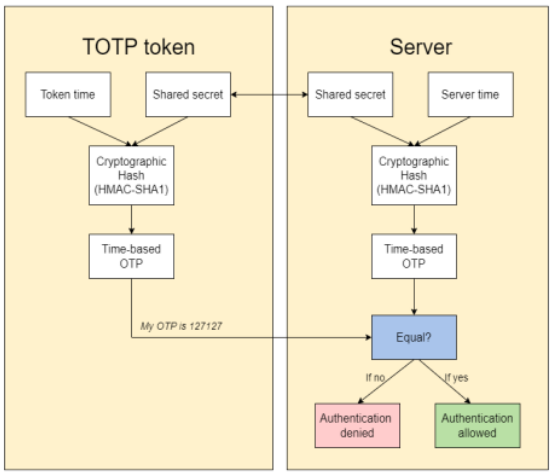

Figure 2: TOTP algorithm

For example, Mariano L. T., etc suggested that the message to be hashed by HMAC in OTP algorithms is thecounter value. For TOTP, this counter is determined by the number of 30-second intervals that have elapsedsince the Unix Epoch. As the result, the HMAC-SHA1 hash is generated using the following function:

SHA1(outer pad+SHA1(inner pad+counter))

The limitations and challenges encountered with this advanced method are Security V/S Trading Resources.The lightweight algorithms are commonly not computationally expensive, but they may offer less security thanstronger cryptographic algorithms. There is a possible trade-off

between having low computational overheadand maintaining a high security level. This makes it hard to balance both. Other than that, is Entropy and Predictability. Simpler mathematical operations could be used by lightweight algorithms which can lower entropy and make OTPs predictable if poorly designed. The impact of this is lower entropy implies that bruteforce and guessing attacks can more easily crack OTPs. Another one is synchronization issues, in working properly, OTP mechanisms, especially time-based (TOTP), need accurate synchronization between the clientdevice and the authentication server. The implication of One-time passwords is subject to network latency, clockdrift, or synchronization errors leading to OTP mismatches that cause legitimate authentication attempts to fail.Lastly are the limited device capabilities, Internet of Things devices often have very weak processing capabilities, memory space, and battery life with some even being power hungry. Sometimes even lightweight algorithms might be too demanding for these most constrained devices.

The TOTP authentication mechanism and inclusion of lightweight crypto algorithms for the time-based OTPs adopted a systematically designed approach to security, efficacy, and convenience. With existing security threats, there are many difficulties in using a symmetric encryption system to improve WSN security [14]. It commences with Requirement Analysis, whereby the available literature and consultative meetings were conducted to identify the standard. During the design phase, the emphasis was placed uponestablishing an effective approach for producing and distributing secret keys, the usage of such lightweightcryptographic algorithms as HMAC-SHA1, and time synchronization capabilities. There was compliance with low-resource devices on implementation and sound coding methodologies and compatibility with initial authentication systems and asymmetric encryption is more complex and requires more computing power than symmetric encryption, but it guarantees authentication and non-repudiation of encryption [14]Sector tests and validations ensured that the system had a high level of security and was functioning well, while optimization work fine-tuned the basic cryptographic algorithms and the time synchronization procedures. The broadband plan included a pilot launch of IoT as well as digital banking and the results that ensued provided the basis for enhancement. Last of all, monitoring and maintenance to guarantee the permanent stability and threat protection with the necessary updates based on the further findings in the sphere of cryptography were developed. Analysis of the above approach therefore led to development of ahighly secure, efficient TOTP system that can be used in numerous applications.

Table1 below shows comparisons between TOTP with lightweight algorithms and the traditional OTPmechanism.

***Table 1**: The comparisons between TOTP with lightweight algorithms and the traditional OTP mechanism*

Metric	Traditional OTP	TOTP with Lightweight Algorithm	Improvement
Security	Moderate	High	Enhanced
Computational efficiency	Low	High	Improved
User friendliness	Moderate	High	Improved
Vulnerability to attacks	High	Low	Reduced

4. RESULTS AND ANALYSIS

This section provides a detailed analysis of how the proposed Time-based One-Time Password (TOTP) authentication mechanism, enhanced with lightweight algorithms, resolves the identified problem statements. It also highlights the specific parts of the current authentication mechanisms that have been improved and discusses the significance of these enhancements.

4.1. Identity Theft Vulnerabilities

- **Problem Statement:** Traditional PIN-based systems are highly susceptible to observation and theft, especially in immersive environments like the metaverse and VR.
- **Resolution with TOTP and Lightweight Algorithms:** TOTP introduces a dynamic, time- sensitive authentication code that changes at regular intervals (usually 30 seconds). The addition of lightweight cryptographic algorithms ensures that these codes are generated and validated efficiently, even on devices with limited processing power. This makes it significantly harder for attackers to steal and use authentication codes, as they must be used within a limited time window.The resilience to observation and theft is thus greatly enhanced [2].

4.2. Manual Data Gathering Risks

- **Problem Statement:** Manual methods of data gathering in industrial environments are error-prone and resource-intensive, leading to potential security breaches and inefficiencies.
- **Resolution with TOTP and Lightweight Algorithms:** Implementing TOTP in systems like machine activation monitoring reduces the dependency on manual data entry. Automated, time- based OTPs ensure that only authorized personnel can access

and interact with machinery,enhancing both security and operational efficiency. The lightweight algorithms ensure that these processes run smoothly without overburdening the system [7].

4.3. Susceptibility to Phishing and Spyware Attacks

- **Problem Statement:** Traditional OTP systems, especially those used in banking applications, arevulnerable to phishing and spyware attacks, posing risks to financial security.
- **Resolution with TOTP and Lightweight Algorithms:** TOTP relies on an algorithm that generatespasswords based on a shared secret and the current time, rather than sending static or pre-defined codes. The use of lightweight algorithms makes these OTPs computationally efficient and secure, mitigating the risks associated with phishing and spyware attacks, as intercepted OTPs quickly become useless [3].

4.4. Security Challenges in Constrained IoT Devices

- **Problem Statement:** IoT devices often lack robust security measures due to constraints like economic and energy consumption limitations.
- **Resolution with TOTP and Lightweight Algorithms:** TOTP can be integrated with lightweight protocols (e.g., MQTT) and secure communication channels (e.g., using blockchain) to enhance security without imposing significant computational or energy overhead. This is especially useful for constrained IoT environments, ensuring secure and efficient authentication [6].

4.5. Identification and Significance of ImprovementsEnhanced Security through Time-based Validity

- **Current Mechanism Limitation:** Static passwords or even traditional OTPs are valid for extendedperiods, making them vulnerable to interception and replay attacks.
- **TOTP Improvement with Lightweight Algorithms:** By limiting the validity of each OTP to a short time window and using lightweight cryptographic algorithms, TOTP reduces the attack surface and the chances of successful interception or replay attacks. This significantly enhances theoverall security of the authentication process [6].
- **Significance:** The time-sensitive nature of TOTP, combined with efficient lightweight algorithms,ensures that even if an OTP is intercepted, it becomes invalid quickly. This reduces the risk of unauthorized access and enhances the security of the system against time-based attacks.

4.6. User-Friendly Implementation

- **Current Mechanism Limitation:** Some advanced authentication methods, like those involving complex hardware tokens or multi-step verification, can be cumbersome for users.
- **TOTP Improvement with Lightweight Algorithms:** TOTP applications are widely available onsmartphones and can be easily synchronized with user accounts. The use of lightweight algorithmsensures that these applications run efficiently, providing a balance between security and usability [8].
- **Significance:** By being easy to implement and use, TOTP with lightweight algorithms encouragesbroader adoption and compliance among users, thereby improving overall security without addingsignificant complexity.

4.7. Compatibility with Existing Systems

- **Current Mechanism Limitation:** Implementing new security measures often requires significantchanges to existing infrastructure.
- **TOTP Improvement with Lightweight Algorithms:** TOTP can be integrated into existing systems with minimal changes. The lightweight nature of the algorithms ensures that the integrationis smooth and does not impose significant computational or energy demands on the system [10].
- **Significance:** This compatibility ensures that organizations can enhance their security posture without significant disruptions or additional investments in new infrastructure.

4.8. Limitations and Challenges of TOTP with Lightweight Algorithms

- **Security vs. Resource Trade-Off**
  - **Challenge:** Lightweight algorithms are often less computationally intensive but may provide lowersecurity compared to more robust cryptographic algorithms.
  - **Impact:** There is a potential trade-off between achieving low computational overhead andmaintaining a high level of security, making it challenging to balance both [12].
- **Entropy and Vulnerability**
  - **Challenge:** Lightweight algorithms might use simpler mathematical operations, which couldpotentially reduce the entropy and make OTPs more predictable if not carefully designed.
  - **Impact:** Lower entropy can make OTPs more vulnerable to brute force and guessing attacks [4].

- **Synchronization Issues**
  - **Challenge:** OTP mechanisms, especially time-based ones (TOTP), require precise synchronization between the client device and the authentication server.
  - **Impact:** Network latency, clock drift, or synchronization errors can lead to OTP mismatches, causing legitimate authentication attempts to fail [11].
- **Limited Device Capabilities**
  - **Challenge:** IoT devices often have extremely limited processing power, memory, and battery life. Even lightweight algorithms can sometimes be too demanding for the most constrained devices.
  - **Impact:** Implementing even the simplest of OTP mechanisms can be challenging on ultra-low-power devices, leading to performance degradation or faster battery depletion [11].

5. DISCUSSION AND RECOMMENDATION

The adoption of Time-Based OTP (TOTP) with lightweight algorithms effectively addresses critical vulnerabilities and inefficiencies in current authentication mechanisms. By generating dynamic, time- sensitive passwords, TOTP significantly reduces the risk of code reuse and interception, thereby enhancing security across various applications, including virtual reality, IoT, and digital banking. The use of lightweight cryptographic algorithms ensures that these security measures can be implemented efficiently, even on devices with limited processing capabilities. This makes TOTP a versatile solution that can be widely adopted across different sectors, providing robust protection against unauthorized access and cyber threats.

However, while TOTP with lightweight algorithms offers substantial improvements, it is not without challenges. Synchronization between client devices and authentication servers remains a critical issue, as any discrepancies can lead to authentication failures. Additionally, there is a delicate balance between maintaining high security levels and ensuring computational efficiency. Lightweight algorithms, while reducing the computational load, may offer less security than more robust cryptographic methods. Addressing these challenges requires continuous optimization and careful design considerations to achieve a balanced approach to security and performance. Future research should focus on enhancing synchronization mechanisms, improving the entropy of lightweight algorithms, and exploring additional applications to validate and expand the use of TOTP in diverse environments.

6. CONCLUSION

In conclusion, the implementation of the Time-Based One-Time Password (TOTP) authentication mechanism enhanced with lightweight cryptographic algorithms presents a significant advancement in addressing the limitations of traditional OTP systems. The dynamic nature of TOTP, generating time- sensitive passwords, greatly reduces the vulnerabilities associated with code reuse and interception, thus enhancing security across various applications, including digital banking, IoT environments, and virtual reality.

Our research demonstrates that lightweight algorithms can be effectively integrated into TOTP systems, ensuring robust security while maintaining efficiency on resource-constrained devices. This balance between security and computational efficiency makes TOTP a viable solution for modern authentication needs, particularly in scenarios where device capabilities are limited.

However, it is essential to acknowledge the challenges and limitations associated with this approach. Synchronization issues between client devices and authentication servers, the trade-off between security strength and computational overhead, and the potential predictability of OTPs generated by simpler mathematical operations are critical areas that require careful consideration and ongoing research.

Overall, the adoption of TOTP with lightweight algorithms provides a promising path forward in the realmof secure and efficient two-factor authentication. Future work should focus on optimizing the synchronization mechanisms, enhancing the entropy of lightweight algorithms, and exploring additional applications to further validate and expand the utility of this advanced authentication method.

7. ACKNOWLEDGEMENTS

This research work is the outcome of a class project in the Computer Science and Information Technologydepartment at Universiti Malaysia Sarawak, Malaysia.

REFERENCES

[1] Aggarwal, N., Kumari, S., Bahl, S., Jain, U., Rathore, N., & Saini, D. Secure One-Time Password Generation Using Shamir's Secret Sharing. Retrieved from www.ijfmr.com

[2] Aparicio, A., Martínez-González, M. M., & Cardeñoso-Payo, V. (2023). App-based detection of vulnerable implementations of OTP SMS APIs in the banking sector. *Wireless Networks*. https://doi.org/10.1007/s11276-023-03455-w

[3] Buccafurri, F., & Romolo, C. (2019). A Blockchain-Based OTP-Authentication Scheme for Constrained IoT Devices Using MQTT. In *ACM International Conference Proceeding Series*. Association for Computing Machinery. https://doi.org/10.1145/3386164.3389095

[4] Catalfamo, A., Ruggeri, A., Celesti, A., Fazio, M., & Villari, M. (2021). A Microservices and Blockchain Based One Time Password (MBB-OTP) Protocol for Security-Enhanced Authentication. In *Proceedings - IEEE Symposium on Computers and Communications*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISCC53001.2021.9631479

[5] Iqbal, A. M. (2012). Evaluation of Research Collaboration Between University and Industry.

[6] Iqbal, A. M., Khan, A. S., & Senin, A. A. (2012). Determination of High Impact Evaluation Metrics for Evaluating the University-Industry Technological Linkage.

[7] Jadhav, P., Gaul, S., Madhwai, A., Nikam, V., Mhalaskar, K., & Deshmukh, M. (2023). A Cutting-Edge Security Solution: OTP-Based Smart Wireless Locking System. In *2023 4th International Conference on Computation, Automation and Knowledge Management, ICCAKM 2023*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCAKM58659.2023.10449610

[8] Kamilah, S., Shahid, A., Fisal, N., Rozeha, A. R., & Abbas, M. (2011).

[9] Khan, A. S. (2012). Medium Access Control Security Mechanism for Mobile Multihop Relay WiMAX Networks.

[10] Khan, A. S., et al. (2010). An Improved Authentication Key Management Scheme for Multihop Relay in IEEE 802.16m Networks.

[11] Khan, R. H., & Miah, J. (2022). Performance Evaluation of a new One-Time Password (OTP) Scheme Using Stochastic Petri Net (SPN). In *2022 IEEE World AI IoT Congress, AIIoT 2022* (pp. 407–412). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AIIoT54504.2022.9817203

[12] Krishna, S. P., Tejasri, D., Soumya, B., Madhuri, M., & Lubna. (2022). Bank Application: One-Time Password Generation. In *Proceedings - International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2022* (pp. 855–859). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICAAIC53929.2022.9792823

[13] Li, P., Pan, L., Chen, F., Hoang, T., & Wang, R. (2023). TOTPAuth: A Time-based One Time Password Authentication Proof-of-Concept against Metaverse User Identity Theft. In *Proceedings - 2023 IEEE International Conference on Metaverse Computing, Networking and Applications, MetaCom 2023* (pp. 662–665). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MetaCom57706.2023.00117

[14] Matelski, S. (2022). Human-Computable OTP Generator as an Alternative of the Two-Factor Authentication. In *ACM International Conference Proceeding Series* (pp. 64–71). Association for Computing Machinery. https://doi.org/10.1145/3528580.3532842

[15] Nisa, N., Khan, A. S., Ahmad, Z., Aqeel, S., Asim, J., & Afzal, S. (2022). Conceptual Review of DoS Attacks in Software Defined Networks.

[16] Saputra, L. K. P., Filiana, A., Rini, M. N. A., Tamtama, G. I. W., Kurniawan, L., & Surya, H. B. (2023). One Time Password Authentication for Machine Activation Monitoring System Based on Wireless Network. In *Proceedings - IEIT 2023: 2023 International Conference on Electrical and Information Technology* (pp. 252–257). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/IEIT59852.2023.10335513

[17] Saqib, R. M., et al. (2022). Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security. *Intelligent Automation & Soft Computing*.

[18] Shankar, T. N., Rakesh, P., Bhargawa Rao, T., Hari Bharadwaj, L., Rakesh, C., & Madhuri, M. L. (2021). Providing Security to Land Record with the Computation of Iris, Blockchain, and One Time Password. In *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021* (pp. 226–231). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCIS51004.2021.9397176

[19] Teffandi, N., Feryputri, N. A. Z., Hasanuddin, M. O., Syafalni, I., & Sutisna, N. (2023). GRAIN Algorithm Implementation for Lightweight Hardware-Based OTP Authentication. In *Proceedings of the International Conference on Electrical Engineering and Informatics*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICEEI59426.2023.10346638

[20] Xu, G., Qiao, Y., Wu, X., Institute of Electrical and Electronics Engineers, Institute of Electrical and Electronics Engineers. Beijing Section, & Zhongguo ke xue yuan. Shenzhen xian jin ji shu yan jiu yuan. (n.d.). Time-based OTP Authentication via Secure Tunnel (TOAST): A Mobile TOTP Scheme Using TLS Seed Exchange and Encrypted Offline Keystore.

Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems

ORIGINALITY REPORT

10%	4%	8%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Chenxi (Cecilia) Li, Tim Lewis. "Negotiation for Meaning Routines in Audio SCMC Interactions", International Journal of Computer-Assisted Language Learning and Teaching, 2018 Publication	1%
2	Sondes Baccouri, Hassene Farhat, Tarek Azzabi, Rabah Attia. "Lightweight authentication scheme based on Elliptic Curve El Gamal", Journal of Information and Telecommunication, 2023 Publication	1%
3	"Image Processing, Electronics and Computers", IOS Press, 2024 Publication	1%
4	Mariano Luis T. Uymatiao, William Emmanuel S. Yu. "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore", 2014 4th IEEE	1%

	International Conference on Information Science and Technology, 2014 Publication	
5	Submitted to Teaching and Learning with Technology Student Paper	1 %
6	securingiot.projectsbyif.com Internet Source	<1 %
7	caisils.unimas.my Internet Source	<1 %
8	napier-repository.worktribe.com Internet Source	<1 %
9	www.al-kindipublisher.com Internet Source	<1 %
10	Siva Raja Sindiramutty, Chong Eng Tan, Wei Wei Goh, Sumathi Balakrishnan, Norhidayah Hamzah, Rehan Akbar. "chapter 11 Securing the Supply Chain", IGI Global, 2024 Publication	<1 %
11	Ayan Banerjee, Chinmoy Ghosh, Satyendra Nath Mandal. "Analysis of V-Net Architecture for Iris Segmentation in Unconstrained Scenarios", SN Computer Science, 2022 Publication	<1 %
12	Submitted to Campbellsville University Student Paper	<1 %

13	hackernoon.com Internet Source	<1%
14	link.springer.com Internet Source	<1%
15	researchr.org Internet Source	<1%
16	"Intelligent Computing", Springer Science and Business Media LLC, 2021 Publication	<1%
17	Submitted to North American University Student Paper	<1%
18	Laurentius Kuncoro Probo Saputra, Agata Filiana, Maria Nila Anggia Rini, Gabriel Indra Widi Tamtama et al. "One Time Password Authentication for Machine Activation Monitoring System Based on Wireless Network", 2023 International Conference on Electrical and Information Technology (IEIT), 2023 Publication	<1%
19	Pengyu Li, Lei Pan, Feifei Chen, Thuong Hoang, Rui Wang. "TOTPAuth: A Time-based One Time Password Authentication Proof-of-Concept against Metaverse User Identity Theft", 2023 IEEE International Conference on	<1%

Metaverse Computing, Networking and Applications (MetaCom), 2023
Publication

20	ijisrt.com Internet Source	<1%
21	mail.jurnal.stmik-yadika.ac.id Internet Source	<1%
22	Sharareh Monfared, Daniel Andrade, Luis Rodrigues, Joao Nuno Silva. "BioALeg - Enabling Biometric Authentication in Legacy Web Sites", 2016 IEEE 35th Symposium on Reliable Distributed Systems Workshops (SRDSW), 2016 Publication	<1%
23	Sławomir Matelski. "Human-Computable OTP Generator as an Alternative of the Two-Factor Authentication", EICC 2022: Proccedings of the European Interdisciplinary Cybersecurity Conference, 2022 Publication	<1%
24	Haqi Khalid, Shaiful Jahari Hashim, Sharifah Mumtazah Syed Ahmad, Fazirulhisyam Hashim, Muhammad Akmal Chaudary. "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles", 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020	<1%

Publication

25	www.iieta.org Internet Source	<1%
26	Nicholas Teffandi, Najmi Az-Zahra Feryputri, Muhammad Ogin Hasanuddin, Infall Syafalni, Nana Sutisna. "GRAIN Algorithm Implementation for Lightweight Hardware-Based OTP Authentication", 2023 International Conference on Electrical Engineering and Informatics (ICEEI), 2023 Publication	<1%
27	Alessio Catalfamo, Armando Ruggeri, Antonio Celesti, Maria Fazio, Massimo Villari. "A Microservices and Blockchain Based One Time Password (MBB-OTP) Protocol for Security-Enhanced Authentication", 2021 IEEE Symposium on Computers and Communications (ISCC), 2021 Publication	<1%
28	H. P. Asha, I. Diana Jeba Jingle. "Chapter 20 One Time Password-Based Two Channel Authentication MechanismUsing Blockchain", Springer Science and Business Media LLC, 2022 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15