DESIGN AND IMPLEMENTATION OF A SITUATION MAPPING SECURITY SYSTEM USING MULTI-FACTOR AUTHENTICATION BASED ON FINGERPRINT BIOMETRICS

Jeki Saputra[1)], Yelin Rocky T Depondoye[2)], Yohanes Dwi Cahyono[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: jekiana2010@gmail.com[1)], d4chiper01@gmail.com[2)], indorana2012@gmail.com[3)]

DESIGN AND IMPLEMENTATION OF A SITUATION MAPPING SECURITY SYSTEM USING MULTI-FACTOR AUTHENTICATION BASED ON FINGERPRINT BIOMETRICS

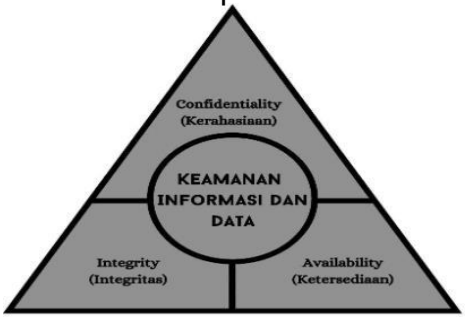
ABSTRACT: This research centers on the development and deployment of a secure situation-mapping framework that integrates Multi-Factor Authentication (MFA) with biometric fingerprinting and the FIDO2 WebAuthn protocol. The project was initiated as a response to the growing sophistication of cyber threats—specifically phishing and unauthorized access—which pose a significant risk to sensitive territorial data.Adopting a Research and Development (R&D) methodology, the study progressed through systematic phases: requirement analysis, architectural design, implementation, and rigorous testing. The core of the system lies in its dual-layered defense, combining traditional credentials (username and password) with advanced biometric verification. To maintain high precision, the fingerprint matching process utilizes minutiae extraction paired with Euclidean distance calculations and rotation transformations. This technical approach ensures that verification remains accurate even when scanning positions are inconsistent.The implementation results demonstrate a marked improvement in both authentication speed and overall security. Furthermore, thorough white-box testing confirms that the architecture is resilient against common vulnerabilities, including SQL Injection and Cross-Site Scripting (XSS). Ultimately, the developed system provides a robust solution for data protection while significantly enhancing the operational efficiency of situation mapping management.

Keywords: Situation Mapping, Multi-Factor Authentication, Fingerprint Biometrics, FIDO2, WebAuthn.

ABSTRAK: Penelitian ini berfokus pada pengembangan sistem keamanan pemetaan situasi yang mengintegrasikan *Multi-Factor Authentication* (MFA) dengan teknologi biometrik sidik jari serta protokol FIDO2 WebAuthn. Langkah ini diambil sebagai respons terhadap meningkatnya ancaman serangan siber, seperti *phishing* dan akses ilegal, yang berisiko membocorkan data teritorial sensitif.Melalui pendekatan *Research and Development* (R&D), tahap pengembangan dimulai dari analisis kebutuhan mendalam, perancangan, hingga pengujian sistem secara menyeluruh. Keunggulan sistem ini terletak pada penggabungan metode login konvensional (nama pengguna dan kata sandi) dengan lapisan verifikasi biometrik. Untuk menjamin akurasi, proses pencocokan sidik jari menerapkan metode ekstraksi *minutiae* yang dikombinasikan dengan perhitungan *Euclidean distance* serta transformasi rotasi. Hal ini memastikan proses verifikasi tetap presisi meskipun terdapat variasi posisi saat pemindaian dilakukan.Hasil implementasi menunjukkan bahwa sistem tidak hanya menawarkan tingkat keamanan yang lebih kokoh, tetapi juga performa autentikasi yang lebih cepat. Berdasarkan pengujian *white-box*, sistem terbukti tangguh dalam menghadapi berbagai kerentanan umum, termasuk *SQL Injection* dan *Cross-Site Scripting* (XSS). Secara keseluruhan, sistem yang dikembangkan berhasil memperkuat proteksi data sekaligus mendukung efektivitas operasional dalam pengelolaan pemetaan situasi.

INTRODUCTION

As digital infrastructure becomes increasingly central to military and governmental operations, the demand for ironclad authentication has never been higher. Traditional security measures—which often rely on a simple combination of usernames and passwords—are no longer sufficient to withstand modern threats. These legacy systems remain highly susceptible to credential theft, sophisticated phishing, and brute-force intrusions, leaving critical systems exposed.In the context of territorial data management and situation-mapping, the stakes are even higher; a single unauthorized entry could lead to catastrophic security breaches. To mitigate these risks, implementing Multi-Factor Authentication (MFA) alongside biometric fingerprinting offers a significantly more resilient defense than standard protocols. This multi-layered approach ensures that access is granted only through verified, physical identity markers.This research addresses these vulnerabilities by developing a security framework that merges the FIDO2 WebAuthn protocol with fingerprint biometrics. The ultimate goal is to build a high-integrity authentication layer specifically tailored to meet the rigorous security requirements of situation-mapping applications, ensuring both data protection and operational trust.



The identification of security requirements is guided by the CIA Triad principle (Confidentiality, Integrity, and Availability). This ensures that territorial data is only accessible to authorized personnel (Confidentiality), remains accurate and unaltered during processing (Integrity), and is consistently accessible for operational needs (Availability).

RESEARCH METHOD

This study employs a Research and Development (R&D) framework, a systematic approach designed to bridge the gap between theoretical security concepts and functional, field-ready applications. The research journey is divided into five critical, interconnected phases:

1. Requirement Analysis & Identification

The process began with an in-depth requirement analysis to establish a solid security baseline. This phase involved conducting structured interviews and field observations aimed at identifying the specific vulnerabilities in existing territorial data management. By gathering data from potential users and security experts, the study established the necessary standards for authentication speed, user accessibility, and data integrity.

2. Multi-Layered System Architecture Design

The design phase focused on constructing a robust defense-in-depth architecture. The system does not rely on a single point of failure; instead, it integrates three core components:

a. Knowledge-based: Standard username and password credentials.
b. Inherence-based: Biometric fingerprint recognition.
c. Protocol-based: The FIDO2 WebAuthn standard, which ensures that cryptographic keys never leave the user's device, effectively neutralizing remote phishing attempts.

3. Cross-Platform Implementation

To ensure operational flexibility, the system was developed using a hybrid approach, making it compatible with both web-based dashboards and mobile applications. This phase involved the integration of hardware-level biometric APIs (such as Android BiometricPrompt or Web Crypto API) to allow the software to communicate securely with the fingerprint sensors on various devices.

4. The Biometric Engine: Minutiae & Euclidean Logic

A significant technical focus was placed on the fingerprint matching algorithm. To handle the "noise" and variability of real-world scans, the study implemented a multi-stage verification process:

a. Minutiae Extraction: Identifying unique ridge endings and bifurcations.
b. Rotation Transformation: Adjusting the input data to

account for different finger

c. Euclidean Distance Calculation: Measuring the spatial relationship between minutiae points to determine a "similarity score." Access is granted only if this score meets a predefined high-precision threshold.

5. Rigorous Security & Reliability Testing

The final stage involved a multi-tiered testing strategy to validate the system's resilience.

a. Functional Testing: Ensuring a seamless user journey from registration to login.
b. White-Box Testing: A "transparent" code review to ensure the internal logic is sound.
c. Vulnerability Assessment: Specifically simulating SQL Injection and Cross-Site Scripting (XSS) attacks to confirm that the database and user sessions remain impenetrable.

RESEARCH RESULTS

The implementation and testing phases of this study have yielded comprehensive data regarding the efficacy and reliability of the developed security solution. The findings are categorized into the following key performance and security indicators:

1. Successful Cross-Platform Deployment and Interoperability

angles.

The development phase successfully realized a unified security framework that synergizes Multi-Factor Authentication (MFA) with biometric fingerprint technology. The system demonstrated a high degree of interoperability, with the FIDO2 WebAuthn protocol functioning consistently and stably across various hardware architectures. This success includes seamless data synchronization between the web-based administrative dashboard and the mobile client application, providing a uniform user experience without compromising security standards at any access point.

2. Strategic Alignment with Information Security Pillars (The CIA Triad)

The system architecture was engineered with a primary focus on the three fundamental pillars of data protection: Confidentiality, Integrity, and Availability. This framework serves as the core evaluative baseline to ensure that territorial data managed within the situation mapping system is shielded from multi-dimensional threats.

[INSERT YOUR CIA TRIAD IMAGE HERE]
Figure 1: The Information Security Framework (CIA Triad) applied as the baseline for system evaluation.

a. Confidentiality: Through the rigorous application of MFA, sensitive territorial data is guaranteed to be accessible only to authorized personnel, effectively closing loopholes for external information leaks.

b. Integrity: The utilization of precision biometric matching algorithms ensures that mapping data cannot be manipulated or altered illegally; any data modification is only possible through valid physical identity verification.
c. Availability: The system is designed to be resilient and accessible at all times to support daily operational needs, ensuring that security barriers do not impede the flow of administrative or field-based workflows.

3. Authentication Performance Optimization and Latency Reduction

Quantitative testing indicates a significant improvement in user access speed. When compared to traditional manual credential entry (username and password), the integration of biometric sensors reduced overall authentication latency dramatically. This time efficiency is crucial in situation mapping management, where operational response speed is a decisive factor, yet it is achieved without compromising the rigorous identity verification procedures.

4. Deep Security Validation and Vulnerability Assessment

Comprehensive white-box testing was conducted to examine every layer of the application's internal logic and source code structure. Technical evaluations confirm that the architecture is resilient against critical cyber exploits. Specifically, the system successfully mitigated risks associated with common yet dangerous attacks, such as SQL Injection and Cross-Site Scripting (XSS), resulting in a "hardened" environment for sensitive data processing.

5. Secure Database Architecture and Cryptographic Protection

Data protection extends beyond the login interface to the backend infrastructure. User profiles and biometric templates are not stored as raw images; instead, they are saved as hashed minutiae data using advanced cryptographic standards. This mechanism provides an additional layer of security; even in the event of a database breach, the original biometric information remains obfuscated and entirely unusable or unreconstructable by attackers for illicit purposes.

Table 1. Comparison of Related Studies

No	References	Narrative	Key Results	Implication
1	Lubis et al. (2025)	Discussed information security challenges in digital financial systems and emphasized the importance of layered security mechanisms.	Highlighted vulnerabilities in single-factor authentication systems.	Reinforces the need for Multi-Factor Authentication (MFA) in sensitive data environments.
2	Agreindra et al. (2024)	Analyzed cybersecurity risks and defense strategies in modern digital infrastructure.	Identified phishing and malware as dominant attack vectors.	Supports the integration of stronger authentication protocols such as FIDO2.
3	WebAuthn & FIDO2 Implementation Studies	Examined passwordless authentication using WebAuthn standards.	Reduced phishing risks and improved authentication reliability.	Validates the use of FIDO2 in secure system development.
4	Biometric Fingerprint Authentication Research	Investigated fingerprint minutiae extraction methods using Euclidean distance and rotation alignment.	Achieved high matching accuracy despite fingerprint position variations.	Demonstrates biometric feasibility for high-security applications.
5	This Research	Integrates MFA, fingerprint biometrics, and WebAuthn FIDO2 into a situation mapping system.	Improved authentication speed and enhanced resistance to SQL Injection and XSS vulnerabilities.	Provides an applied security model for military-based situation mapping systems.

DISCUSSION

The findings of this study underscore a pivotal shift from traditional security models to a more resilient, biometric-centric architecture. The following points elaborate on the technical implications and the strategic value of the integrated system:

1. The Evolutionary Leap from Conventional Credentials

The integration of Multi-Factor Authentication (MFA) with fingerprint biometrics represents a significant advancement over legacy systems. Traditional methods, which rely solely on "something you know" (passwords), are inherently flawed due to human tendencies toward weak password selection and the ease of credential theft. By incorporating "something you are" through biometric verification, the system achieves uniqueness and non-repudiation. Unlike a password, a biometric template cannot be shared, forgotten, or easily duplicated, ensuring that the person accessing the situation mapping data is indeed the authorized individual.

2. Phishing Resilience via FIDO2 WebAuthn

A standout feature of this implementation is the use of the FIDO2 WebAuthn protocol. This protocol effectively neutralizes one of the most common cyber threats: phishing. Because FIDO2 binds the authentication process to a specific registered device and a unique origin (domain), a remote attacker cannot intercept and reuse credentials on a fraudulent site. This "origin-binding" creates a hardware-level trust anchor, ensuring that even if a user is tricked into visiting a malicious link, the authentication handshake will fail, thereby safeguarding sensitive territorial information.

3. Addressing Environmental and Physical Constraints

Despite the high security ceiling, the study acknowledges practical limitations inherent in biometric technology. Environmental factors—such as suboptimal lighting for scanners, moisture, or physical damage to a user's fingertips—can result in higher False Rejection Rates (FRR). These "noise" variables can hinder scanning quality and overall system accuracy. Recognizing these challenges is crucial for real-world deployment, especially in rugged or military environments where perfect scanning conditions are not always guaranteed.

4. Strategic Pathways for Future Enhancement

To further fortify the system and improve the user experience, future iterations should prioritize the following enhancements:

a. Algorithmic Refinement: Transitioning to more sophisticated deep-learning-based minutiae extraction could improve accuracy in cases of poor image quality or partial fingerprint scans.
b. Adaptive Authentication Layers: Introducing a fallback mechanism, such as a Time-based One-Time Password (TOTP) or push notifications, would ensure system availability when biometric sensors are unavailable or if a user's physical condition prevents a successful scan.
c. Liveness Detection: Incorporating "anti-spoofing" or liveness detection would add another layer of protection against sophisticated physical attacks, such as high-resolution fingerprint replicas.

CONCLUSION

The primary objective of this research—to architect and deploy a robust security framework for situation mapping—has been successfully achieved. By integrating Multi-Factor Authentication (MFA) with biometric fingerprinting and the FIDO2 WebAuthn protocol, this study establishes a high-integrity defense mechanism tailored for sensitive territorial data management.

The implementation of this system marks a significant improvement

over traditional, single-factor authentication methods. The results demonstrate that the synergy between physical biometrics and cryptographic hardware-bound protocols not only fortifies the system against sophisticated cyber threats—such as phishing and credential theft—but also enhances overall operational effectiveness. Through the reduction of authentication latency and the mitigation of common vulnerabilities like SQL Injection and XSS, the system provides a secure yet efficient environment for real-time situational awareness.

Moving forward, while the current framework provides a formidable barrier against unauthorized access, future development should aim to further diversify the authentication landscape. Expanding the system to include additional layers, such as adaptive Time-based One-Time Passwords (TOTP) or behavior-based analytics, would provide greater flexibility. Furthermore, conducting broader testing across diverse environmental conditions and larger user groups will be essential to refining the minutiae extraction algorithms and ensuring the system's long-term resilience in varied field operations.

REFERENCES

Abdullah Mubarak Lubis, Gladis Jelita, Syafira Okta Vionna Wirya, & Nurbaiti Nurbaiti. (2025).

Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah. https://journal.aptii.or.id/index.php/Switch/article/view/344

Agreindra, M., Yopi, H., Akbar, H., Mahardika, F., Hidayatul, Y., & Link, A. (2024). *Keamanan Teknologi Informasi: Teori, Risiko, dan Strategi Pertahanan di Era Digital*. https://ebook.lppmunsap.org/index.php/books/article/view/6

Ahmad Yusroni1, A. (2022). Implementasi Teknologi Cloud Computing Pada PT Zurich Topas Life Jakarta. In *Jurnal Sistem Informasi dan* (Vol. 2, Issue 1) https://jurnal.bsi.ac.id/index.php/simpatik/article/view/1110/830

Anggi Putriana. (2023). *Implementasi Teknologi Biometrik Pada Mobile Banking Bank Syariah Indonesia (Studi kasus pada Bank Syariah Indonesia KC Bengkulu S Parman 1)*. https://ejournal.uinfasbengkulu.ac.id/index.php/alilmi/article/view/6894/4510

Atmawijaya, R., & Radiyah, U. (2024). *Perancangan Autentikasi Multi Faktor Dengan Pengenalan Wajah Dan Fido (Fast Identity Online)*. https://ejournal.nusamandiri.ac.id/index.php/inti/article/view/5263/1200

Dr.A.Shaji George. (2024). *The Dawn of Passkeys: Evaluating a Passwordless Future*. https://puirp.com/index.php/research/article/view/44/38

Fakhrur Rozi. (2024). *Perancangan Sistem Penyediaan Stok Darah Dalam Blood Supply Chain Management Berbasis Blockchain Pada Pmi Sleman Yogyakarta*. https://dspace.uii.ac.id/bitstream/handle/123456789/51042/19522306.pdf?sequence=1&isAllowed=y

Fauzi, A., Akbar, R., Rizkha, A., Tamiya Putri, S., Fadhilah, I., Putri Iskandar, N., & Ngurah Agung, I. G. (2023). *Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna*. https://www.researchgate.net/profile/Dr-Fauzi/publication/373017346_Keamanan_Cyber_dan_Peretasan_Etis_Pentingnya_Melindungi_Data_Pengguna/links/64d45a37b684851d3d94c5c8/Keamanan-Cyber-dan-Peretasan-Etis-Pentingnya-Melindungi-Data-Pengguna.pdf

Febrian Aska, M., pratama Putta, D., & Julyana Magdalena Sinambela, C. (2024). *Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital*. *5*. https://ejurnal.ubharajaya.ac.id/index.php/jiforty/article/view/3423/2061

Florian M. Farke, R. U. B. L. L. tracekey solutions G. T. S. P. M. and M. D. R. U. B. (2020). *You still use the password after all – Exploring FIDO2 Security Keys in a Small Company*. https://www.usenix.org/system/files/soups2020-farke.pdf

Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (2024). *Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan*. https://siberpublisher.org/index.php/JKMT/article/view/160/115

Jannah, M., Faris Hidayat, M., Agustiyyani, M., Wira Buana, P., & Purwani, F. (2024). *Implementation Of Biometric Authentication To Enhance Security And Privacy Of Digital Wallet Users*. https://idm.or.id/JSCR/index.php/JSCR/article/view/606/488

Khairun Nisa, V., & Dompak, T. (2024). *Perbandingan Pembuatan Kartu Identitas Warga Negara Indonesia dan Singapura*. https://ejournal.upbatam.ac.id/index.php/prosiding/article/view/9381/3894

Mohammed Aziz Al Kabir. (2024). *Adaptive Risk-based Passwordless Authentication: A FIDO2 Integrated Approach for Enhanced Security and Usability*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4795401

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). *Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (LITERATURE REVIEW SIM)*. https://pdfs.semanticscholar.org/ef1e/a134ce5cda0e8c343209a330176c6ea96f34.pdf

Ou, H. H., Pan, C. H., Tseng, Y. M., & Lin, I. C. (2024). *Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security*. *9*. https://www.mdpi.com/2076-3417/14/9/3551

Peizhou Chen. (2024). *Vulnerability Testing for WebAuthn*. https://essay.utwente.nl/98532/1/Chen_MA_EEMCS.pdf

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). *Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering)*. *6*. https://journal.stmiki.ac.id/index.php/jpni/article/view/1097/834

Putri, C. A., Anwar, R. K., Amar, S. C. D., & Rukmana, E. N. (2024). *Keamanan Informasi dan Privasi Pengguna dalam Layanan Perpustakaan Digital*. https://ejournal.perpusnas.go.id/mp/article/view/5317/1473

Rabbani, K. A., Saputra, L., & Louisa, G. B. (2021). *Rekonstruksi Syarat Sah Perjanjian Yang Terdapat di dalam Peraturan Pemerintah Nomor 80 Tahun 2019 Lex Specialis Terhadap Pasal 1320 Kitab Undang-Undang Hukum Perdata Sebagai Ketentuan Lex Generalis*. https://journal.unnes.ac.id/sju/ipmhi/article/view/53270/20901

Rahmawati, D., Viendyasari, M., Lumakto Rienzy Kholifatur, G., Anindhita, W., Ameliah Syavia Bachna, R., Adienda, A., Indang Trihandini, D., Rer Nat Rosari Saleh, Mk., Ruslan Ramli, M., Bachtiar, Y. A., & Siregar, B. (2024). *WASPADA KEJAHATAN PHISHING ATTACK!* https://repository-penerbitlitnus.co.id/id/eprint/248/1/WASPADA%20KEJAHATAN%20PHISHING%20ATTACK!.pdf

Reyhan Duezguen. (2022). *SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays*. https://dl.acm.org/doi/pdf/10.1145/3538969.3539011

Satriyawan, H., & Susanto, S. (2023). *Optimasi Keamanan Smart GridMelalui Autentikasi Dua Lapis: Meningkatkan Efisiensi dan Privasi dalam Era Digital*. https://restikom.nusaputra.ac.id/article/view/254/109

Sharma, S. K., Kumar, A., Ashtagi, R., & Jain, R. (2023). *OCA: An intelligent model for improving security breach of biometric based authentication systems*. https://scholar.google.com/scholar?hl=id&as_sdt=0%2C5&q=OCA%3A+An+intelligent+model+for+improving+security+breach+of+biometric+based+authentication+systems%2C%E2%80%9D+Journal+of+Discrete+Mathematical+Sciences+and+Cryptography&btnG=

Siti Mutia Kosassy. (2025). *Analisis Transformasi Kualitas Pelayanan Berbasis Digital Di Era Vuca*. https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/40927/26191

Tantrinesia[1], M., Amelia[2], L. F., & Sidarwaya, H. A. (2023). *Prosiding Seminar Nasional Pengaruh M-banking Terhadap Pola Belanja Masyarakat di Surabaya*. https://scholar.google.com/scholar?hl=id&as_sdt=0%2C5&q=Prosiding+Seminar+Nasional+Pengaruh+M-banking+Terhadap+Pola+Belanja+Masyarakat+di+Surabaya&btnG=

Timothy Subekti. (2024). *Analisis Implementasi Enkripsi Biometrik-AES pada Environment Variable dalam Pengembangan Perangkat Lunak*. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2023-2024/Makalah/Makalajh-II4031-Kriptokoding-2024%20(5).pdf

Tri Ginanjar Laksana1, S. M. (2024). *Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan*. https://journal.admi.or.id/index.php/JUKIM/article/view/1143/1308

Ujung, A. M., Irwan, M., & Nasution, P. (2023). *Pentingnya Sistem Keamanan Database untuk melindungi data pribadi*. https://jurnal.unidha.ac.id/index.php/jiska/article/view/929/546

Unggul Budi Astowo. (2023). *Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid*. https://j-innovative.org/index.php/Innovative/article/view/6908/4846

Victor Benny Alexsius Pardosi, B. D. F. N. dan A. Y. V. (2024). *Sistem Keamanan Informasi*. http://repository.undha.ac.id/1645/1/Sistem%20Keamanan%20Informasi.pdf

Wijayanto, H. (2024). *Aplikasi Verifikasi Sertifikat Berbasis Website Menggunakan Blockchain*. https://journal.ukrim.ac.id/index.php/JIF/article/view/586/438

Yusuf Daeng, J. L. K. M. R. P. P. R. N. S. I. V. (2023). *Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia*. https://j-innovative.org/index.php/Innovative/article/view/6376/4461

Zul Khaidir Kadir. (2025). *Volume 12 Nomor 2 Februari 2025 Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse*. https://journalstih.amsir.ac.id/index.php/julia/article/view/633/352