Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Implementation of Zero Knowledge Proof Technology for User Security Verification in Web-Based Systems

Octara Pribadi[1*], Johanes Terang Kita Perangin Angin[2], Erick[3]

[1,3]Informatics Engineering Study Program, STMIK Time, Medan, Indonesia
[2]Information Systems Study Program, STMIK Time, Medan, Indonesia
octarapribadi@gmail.com[1], timejohanes@gmail.com[2], erickzlai@gmail.com[3]*

Abstract

The development of information technology has driven the need for stronger security systems and guaranteed privacy on web-based platforms. Traditional verification methods such as passwords and two-factor authentication are increasingly seen as insufficient in facing the growing complexity of cyber threats. Zero-Knowledge Proof (ZKP) emerges as an alternative solution that enables identity verification without revealing sensitive information. This research aims to implement ZKP technology in web-based systems to enhance user security and privacy. The method involves the implementation of a simple XOR-based ZKP algorithm to prove identity without disclosing personal data, as well as a three-step verification mechanism between the verifier and the prover. Implementation results show that the system can prevent attacks such as man-in-the-middle and replay attacks, while maintaining data confidentiality during the authentication process. This study also identifies challenges in system efficiency and verification process integrity and offers technical solutions to support broader ZKP integration in digital platforms. Thus, the use of ZKP in web-based systems holds great potential to improve user trust and security in the digital era.

Keywords: *Zero-Knowledge Proof, user security, data privacy, web-based systems, authentication*

1. Introduction

The rapid transformation of information technology has impacted many sectors, including user protection systems in web-based applications. The transition from traditional verification methods such as passwords and two-factor authentication to more advanced and secure solutions like Zero-Knowledge Proof (ZKP) is gaining attention. According to a study [1], the use of ZKP technology offers several advantages, such as enhanced data privacy, reduced identity theft risk, and easier user access. Additionally, this technology is expected to increase user trust in the security of digital platforms across various online activities such as banking transactions, e-commerce, and healthcare services. Although ZKP implementation is still in its early stages, it shows great potential in strengthening security and privacy in the digital ecosystem.

Despite its advantages, implementing Zero-Knowledge Proof (ZKP) technology in user security verification on web-based systems faces several challenges. One major issue is the complexity of implementing ZKP efficiently without sacrificing system performance. Research [2] shows that while ZKP can reduce data theft risks and improve privacy, it remains vulnerable to cyberattacks such as man-in-the-middle attacks and eavesdropping during authentication. Other challenges include ensuring transparency in the verification process, where users must be confident that their identities are properly verified without any sensitive information leakage. Concerns over integrity and reliability of ZKP-based systems pose a barrier to its widespread adoption across sectors such as banking, e-commerce, and other digital services.

To address security and privacy issues in web-based systems, several solutions have been proposed by researchers in Indonesia. One promising approach is the use of Zero-Knowledge Proof (ZKP) technology. A study by [3] shows that ZKP can verify user identities without revealing sensitive information, thereby preserving user data confidentiality. This technology allows transaction or action verification without disclosing personal data, which is vital for maintaining privacy and preventing identity theft. In the context of user security, [4] stated that ZKP implementation can increase public trust in system security. They demonstrated that with ZKP, the verification process can be conducted by third parties without accessing sensitive data, which is crucial in preventing misuse. Furthermore, [5] highlighted that integrating ZKP into web-based systems can enhance overall security. With ZKP, user authentication can be performed without revealing their true identity, thereby reducing the risk of cyberattacks and data theft. The study also emphasized the importance of a strong infrastructure to support ZKP implementation, involving advanced computing and encryption.

Given the increasingly complex development of security technology and the various issues in maintaining user privacy and security in web-based systems, the authors were motivated to explore a technology-based solution to address these challenges. The use of Zero-Knowledge Proof technology in security verification systems offers great potential to enhance user data protection and maintain the confidentiality of personal information. Therefore, the authors selected this issue for their final project entitled: "Implementation of Zero-Knowledge Proof Technology for User Security Verification in Web-Based Systems." This research is expected to make a tangible contribution to the development of more secure and reliable digital security systems, as well as to increase user trust in online platforms in the future.

2. Theoretical Review

2.1. Definition of Design

The term "design" originates from the verb "to design," which means to plan or prepare something. "Designing" as a noun refers to a process. In certain contexts, "design and build" can also refer to the activity of creating a plan or layout [6].
Design is the initial stage of the creative process that involves processing random ideas or concepts into a structured arrangement with a specific function. This includes drawing, designing, and sketching to integrate elements into a functional whole [7].

2.2. Definition of Application

An application is a computer-based software program used to process data and perform specific tasks according to user needs. The word "application" itself originates from English, meaning the act of applying or using [6].In general, an application is a program designed to meet specific user needs in achieving specific goals. Within information systems, an application supports operations and organizational activities, including the management of hardware, software, and data [8].Applications are also used to assist various human activities, ranging from buying and selling transactions, public services, to entertainment such as games. Some packaged applications are referred to as "application suites" [9].Meanwhile, the system design process is the activity of detailing how the system will work. The goal is to produce software that meets user needs [10][11][12].

2.3. Cryptography

Cryptography comes from the Greek words "crypto" meaning hidden and "graphia" meaning writing. Generally, cryptography is the science and art of securing messages by disguising their content so that only authorized parties can read them [13].In cryptography, the original message (plaintext) is transformed into an encrypted form (ciphertext) through encryption. To revert ciphertext back to plaintext, a decryption process is used [14].Security in the transmission and storage of information is crucial to prevent unauthorized access. Therefore, cryptography plays a vital role in maintaining the confidentiality and integrity of data [15].

2.3. Zero Knowledge Proof

According to the Oxford Dictionary, cryptography involves encoding messages using special characters or specific methods so that only parties with the secret key can understand them. This ensures data confidentiality during information transmission [16].Zero-Knowledge Proof (ZKP) is a cryptographic concept that allows someone to prove the truth of a statement to another party without revealing the underlying information. In practice, the prover sends a statement to the verifier, and with the help of a randomizer, the verifier can confirm the statement's validity without knowing the secret data [17].ZKP is widely used in authentication protocols that prioritize security without data leakage. Algorithms using this principle include Feige-Fiat-Shamir, Guillou-Quisquater, and Schnorr. These algorithms use private and public keys, where prime numbers form the basis for generating public keys. To ensure that the numbers used are prime, testing methods such as Rabin-Miller are applied [16].

3. Method

A diagram illustrating how Zero-Knowledge Proof works is shown in Figure 1:

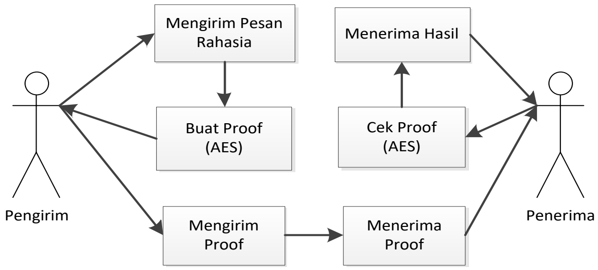


Fig. 1: ZKP Work Diagram

ZKP Work Diagram Explanation:

a. Sending Secret Message by Sender
Before verification begins, the sender prepares a secret message that will serve as the basis for the ZKP. This message may contain important data or identity details to be validated without direct disclosure.

b. Generating Proof Using AES Algorithm
The sender uses an encryption algorithm, such as AES, to generate proof based on the secret message. This ensures that the proof contains valid information verifiable without revealing the original message.

c. Sending Proof to Receiver
Once proof is generated, it is sent to the receiver over a secure channel. This proof is central to the ZKP process.

d. Proof Reception by Receiver
The receiver receives the proof and prepares for verification to confirm its validity without learning the secret message.

e. Proof Validation Using AES Algorithm
The receiver uses the same encryption algorithm (AES) to validate the proof. The process verifies proof validity without access to keys or confidential information.

f. Verification Result Received by Receiver
If verification is successful, the receiver receives a result indicating proof validity. This forms the basis for further steps like data transfer or decryption.

g. Additional Security via ZKP Protocol
ZKP ensures that both sender and receiver share only valid proof without disclosing sensitive information like encryption keys or original messages.

To analyze system components, the authors use a use-case diagram, shown in Figure 2.

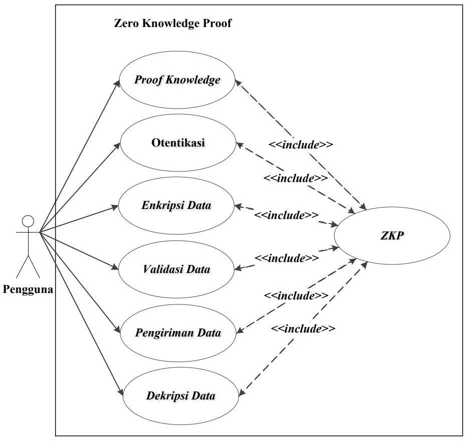


Fig. 2: Use-Case Diagram

An activity diagram describes the workflows of system operations. Below are diagrams for encryption and decryption processes.

1. **Encryption Activity Diagram**
   The user selects encryption, inputs text, and the system processes and returns the output.

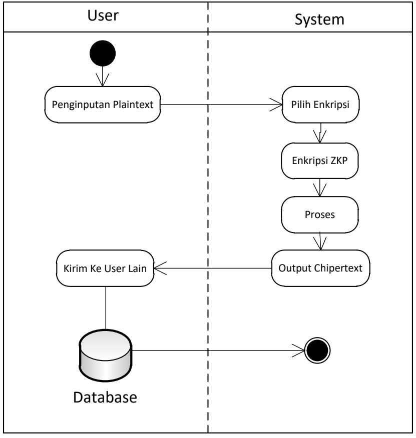


Fig. 3: Encryption Process Activity Diagram

2. ***Decryption Activity Diagram***

The user selects decryption, and the system automatically runs and displays the result.

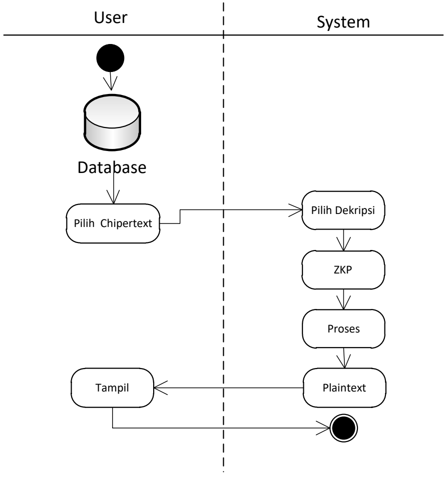


Fig. 4: Decryption Process Activity Diagram

4. Results

The interface designs produced include:

1. Login Interface

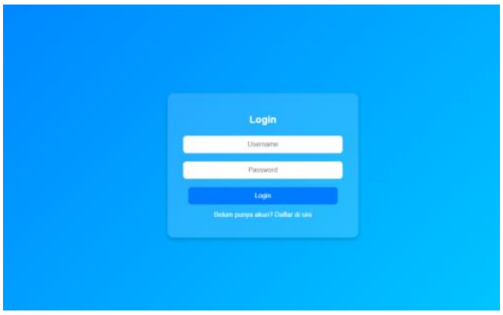
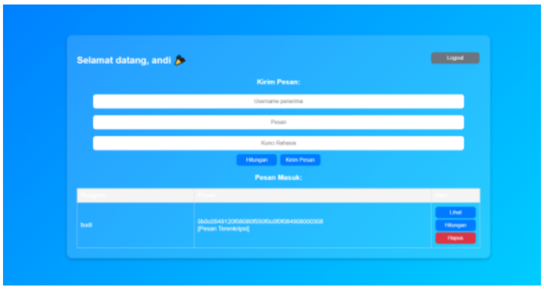


Fig. 5: Login Interface

Contains title, username/password fields, login button, and register link.

2. Dashboard Interface



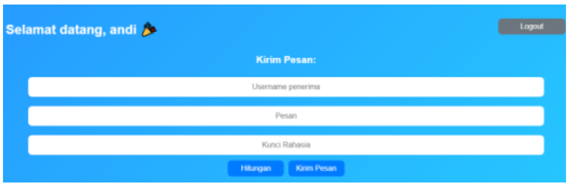
Selamat datang, andi 🎉

Pengirim	Pesan	Aksi
budi	0b0c0549120f06060f550f0c0f0f064908000308 [Pesan Terenkripsi]	Lihat Hitungan Hapus

Fig. 6: Dashboard Interface

Displays a welcome message, form to send encrypted messages, and list of incoming messages with actions.

3. Send Message Interface

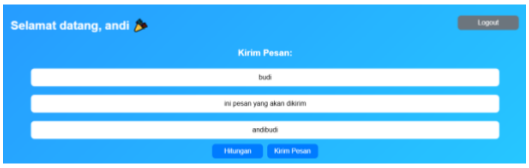


Selamat datang, andi 🎉

Fig. 7: Send Message Interface

Includes fields for recipient username, message content, secret key, and buttons to encrypt and send.

4. Data Example Interface



Selamat datang, andi 🎉

budi

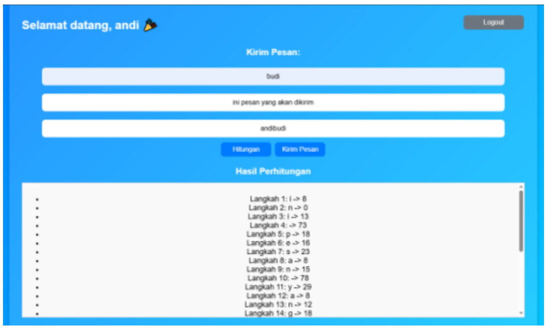
ini pesan yang akan dikirim

andibudi

Fig. 8: Data Example Interface

Shows the result of the encryption calculation.

5. Calculation Example Interface



Selamat datang, andi 🎉

budi

ini pesan yang akan dikirim

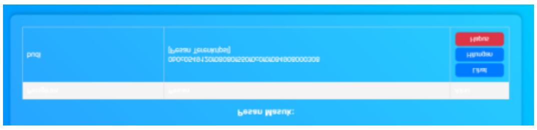
andibudi

- Langkah 1: i -> 8
- Langkah 2: n -> 0
- Langkah 3: i -> 13
- Langkah 4: -> 73
- Langkah 5: p -> 18
- Langkah 6: e -> 16
- Langkah 7: s -> 23
- Langkah 8: a -> 8
- Langkah 9: n -> 15
- Langkah 10: -> 78
- Langkah 11: y -> 29
- Langkah 12: a -> 8
- Langkah 13: n -> 12
- Langkah 14: g -> 18

Fig. 9: Calculation Example Interface

Displays letter-by-letter encryption results.

6. Inbox Interface



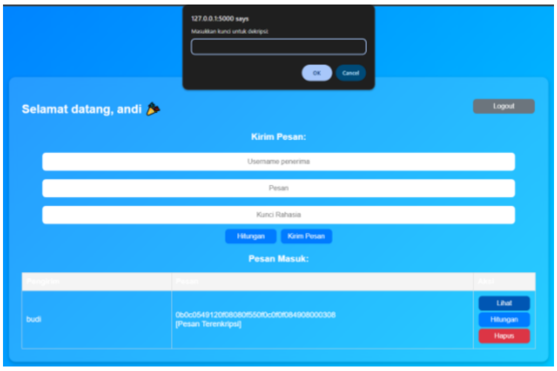
Pesan Masuk:

Pengirim	Pesan	Aksi
budi	0b0c0549120f08080f550f0c0f0f08490800030 8 [Pesan Terenkripsi]	Lihat Hitungan Hapus

Fig. 10: Inbox Interface

Lists received messages with options to view, decrypt, and delete.

7. Password Input Interface



127.0.0.1:5000 says

Masukkan kunci untuk dekripsi:

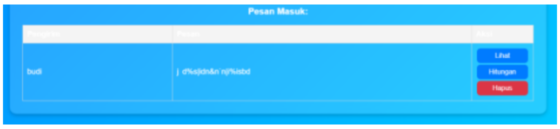
Pesan Masuk:

Pengirim	Pesan	Aksi
budi	0b0c0549120f08080f550f0c0f0f08490800030 8 [Pesan Terenkripsi]	Lihat Hitungan Hapus

Fig. 11: Password Input Interface

Prompts users to enter password before encryption.

8. Incorrect Password Message Interface



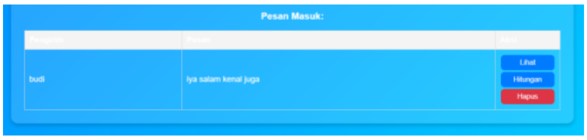
Pesan Masuk:

Pengirim	Pesan	Aksi
budi	j d%sjldn&n`njl%istxd	Lihat Hitungan Hapus

Fig. 12: Incorrect Password Interface

Displays incorrect decryption result if password is wrong.

9. Correct Password Message Interface



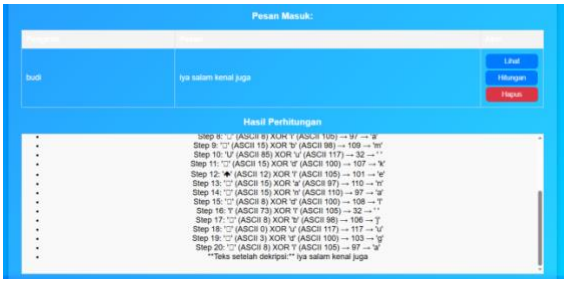
Pesan Masuk:

Pengirim	Pesan	Aksi
budi	iya salam kenal juga	Lihat Hitungan Hapus

Fig. 13: Correct Password Interface

Shows correct decrypted message if the password is valid.

10. Decryption Calculation Interface



Pesan Masuk:

Pengirim	Pesan	Aksi
budi	iya salam kenal juga	Lihat Hitungan Hapus

Hasil Perhitungan

```
• Step 8: '□' (ASCII 8) XOR 'i' (ASCII 105) → 97 → 'a'
• Step 9: '□' (ASCII 15) XOR 'b' (ASCII 98) → 109 → 'm'
• Step 10: 'U' (ASCII 85) XOR 'u' (ASCII 117) → 32 → ' '
• Step 11: '□' (ASCII 15) XOR 'd' (ASCII 100) → 107 → 'k'
• Step 12: '♠' (ASCII 12) XOR 'i' (ASCII 105) → 101 → 'e'
• Step 13: '□' (ASCII 15) XOR 'a' (ASCII 97) → 110 → 'n'
• Step 14: '□' (ASCII 15) XOR 'n' (ASCII 110) → 97 → 'a'
• Step 15: '□' (ASCII 8) XOR 'd' (ASCII 100) → 108 → 'l'
• Step 16: 'I' (ASCII 73) XOR 'i' (ASCII 105) → 32 → ' '
• Step 17: '□' (ASCII 8) XOR 'b' (ASCII 98) → 106 → 'j'
• Step 18: '□' (ASCII 0) XOR 'u' (ASCII 117) → 117 → 'u'
• Step 19: '□' (ASCII 3) XOR 'd' (ASCII 100) → 103 → 'g'
• Step 20: '□' (ASCII 8) XOR 'i' (ASCII 105) → 97 → 'a'
• **Teks setelah dekripsi:** iya salam kenal juga
```

Fig. 14: Decryption Calculation Interface

Shows per-letter decryption results.

5. Conclusion

1) The system successfully integrated Zero-Knowledge Proof (ZKP) technology to enhance user data security and privacy without sacrificing performance. Identity verification is done without disclosing sensitive information, in line with ZKP principles.
2) ZKP implementation in web-based systems can prevent attacks like man-in-the-middle and replay attacks. The three-round interaction mechanism between verifier and prover enhances authentication security.
3) Technical challenges such as algorithm complexity, key management, and communication synchronization were addressed through separate session handling and simple XOR algorithm for efficient encryption-decryption.

Acknowledgments

The author wishes to thank the following individuals and institutions:

1) Mr. Octara Pribadi, M.Kom., as First Supervisor.
2) Mr. Johanes Terang Kita Perangin Angin, S.Kom., M.TI., as Second Supervisor.
3) Mr. Simon Kangga Lee, Chairman of STMIK TIME Foundation, Medan.
4) Dr. Edi Wijaya, S.Kom., M.Kom., M.M., Head of STMIK TIME Medan.
5) Mr. Robet, M.Kom., Head of Informatics Engineering Department, STMIK TIME Medan.
6) Mr. Hendri, M.Kom., Vice Chairman I of Academic Affairs, STMIK TIME Medan.
7) All lecturers of STMIK TIME Medan for their guidance during the academic journey.
8) Special thanks to parents, family, and beloved partner for their physical and emotional support.
9) Friends and colleagues at STMIK TIME for their encouragement, critiques, and suggestions.
10) All parties who contributed to the completion of this thesis.

References

[1] et al. Setiawan, A., “Implementasi Sistem E-Voting dalam Pemilihan Umum di Indonesia,” J. Inspirasi, 2021.

[2] et al. Santoso, D., “Tantangan Keamanan pada Sistem E-Voting di Indonesia,” J. Manaj. dan Teknol. Inf., 2020.

[3] S. et Al., “Pemanfaatan Zero-Knowledge Proof untuk Meningkatkan Keamanan dan Transparansi pada Sistem E-Voting,” J. Infotech, 2021.

[4] P. et Al., “Implementasi Zero-Knowledge Proof dalam Sistem E-Voting untuk Meningkatkan Transparansi dan Kepercayaan Publik,” J. Tek. Inform., 2020.

[5] H. et Al., “Integrasi Zero-Knowledge Proof dalam Sistem E-Voting untuk Meningkatkan Keamanan,” J. Tek. Telekomun. dan Komput., 2020.

[6] R. Y. F. Nurul Samania, Nirsal, “Rancang Bangun Aplikasi E-VOTING Pemilihan Ketua Umum Himpunan Mahasiswa Informatika (HMTI) UNIVERSITAS COKROAMINOTO PALOPO Berbasis WEBSITE,” Eng. Constr. Archit. Manag., vol. 25, no. 1, pp. 1–9, 2020.

[7] E. A. Trianto and A. Yulianeu, “Perancangan Sistem Informasi Pembayaran Abodemen di UPTD Pasar Rajadesa,” Jumantika Tek. Inform. STMIK DCI, 2018.

[8] A. Ni Made, “Analisa dan Perancangan Aplikasi Pembelajaran Bahasa Inggris Dasar Berbasis Android,” J. IKRAITH-INFORMATIKA, vol. 1, no. 3, pp. 107–115, 2020.

[9] F. A. Bukharla and N. Nursyirwan, “Perancangan Aplikasi Android Berbasis Mobile Oleh-Oleh Khas Minangkabau (Minang Pedia),” Gorga J. Seni Rupa, 2020.

[10] Rahmat Gunawan, Arif Maulana Yusuf, and Lysa Nopitasari, “Rancang Bangun Sistem Presensi Mahasiswa Dengan Menggunakan Qr Code Berbasis Android,” Elkom J. Elektron. dan Komput., vol. 14, no. 1, pp. 47–58, 2021.

[11] N. Azis, G. Pribadi, and M. S. Nurcahya, “Aplikasi Pembelajaran Bahasa Inggris Dasar Berbasis Android,” IKRA-ITH Inform., vol. 4, 2020.

[12] M. Ridwan, D. Wiguna, and A. Rusmardiana, “Perancangan Aplikasi Edukasi Pengenalan Lagu Daerah di Indonesia Berbasis Android,” J. Ris. dan Apl. Mhs. Inform., vol. 2, no. 04, 2021.

[13] U. Wahyuningsih et al., “Analisis Proses Enkripsi Algoritma Kriptografi Modern Advanced Encryption Standard (Aes),” J. Adijaya Multidisiplin, vol. 1, no. 2, pp. 380–387, 2023.

[14] Z. Arif and A. Nurokhman, “Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi,” J. Teknol. Sist. Inf., vol. 4, no. 2, pp. 394–405, 2023.

[15] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, “Kriptografi dan Penerapannya Dalam Sistem Keamanan Data,” J. Media Inform., vol. 4, no. 2, pp. 90–93, 2023.

[16] R. Toyib and Y. Darnita, “Pengamanan Data Teks Dengan Menggunakan Algoritma Zero-Knowledge Proof,” J. Media Infotama, vol. 16, no. 1, 2020.

[17] M. F. Abidin, A. Tarigan, and L. Prananingrum, “Perancangan Dan Implementasi Smart Contract Pada Sistem Verifikasi Dokumen Berbasis Zero Knowledge Proof (Zkp) Pada Blockchain Polygon,” J. Ilm. Inform. Komput., vol. 28, no. 2, pp. 100–111, 2023.