HANIF
Journal of Information Systems
https://journal.ilmubersama.com/index.php/hanif

Click here and write your Article Category

Blockchain Integration in Fintech: A Framework for Secure and Transparent Digital Transactions

Surya Guntur[1], Surya Wisada Dachi[2], Willy Yusnandar[3]*

[1]*Department of Informatics Management, Politeknik Ganesha, Medan, 20237, North Sumatra, Indonesia*
[2] *Department of Mathematics Education, Faculty of Teacher Training and Education, Universitas Muhammadiyah Sumatera Utara, Medan, 20238, North Sumatra, Indonesia*
[3] *Department of Management, Faculty of Economics and Business, Universitas Muhammadiyah Sumatera Utara, Medan, 20238, North Sumatra, Indonesia*

ARTICLE INFORMATION

Received: February 00, 00
Revised: March 00, 00
Available Online: April 00, 00

KEYWORDS

Blockchain; Fintech; Data Security; Transparency; Digital Transactions

CORRESPONDENCE

Phone: +6282363800909
E-mail: guntur@polgan.ac.id

A B S T R A C T

The rapid growth of financial technology (FinTech) has transformed digital payment services by providing faster and more accessible financial transactions. However, concerns regarding data security, transaction transparency, fraud, and centralized control remain significant challenges. Blockchain technology has emerged as a promising solution due to its decentralized architecture, cryptographic security, immutability, and transparent transaction records. This study proposes a blockchain integration framework to enhance the security, transparency, and efficiency of digital transactions within FinTech ecosystems. The proposed framework consists of five layers: user application, application programming interface (API), smart contract, blockchain network, and distributed data storage. A prototype was developed using a private blockchain architecture with smart contracts to automate transaction validation and verification. The framework was evaluated through functional testing, security analysis, transaction throughput, latency measurement, and scalability assessment under simulated transaction loads. Experimental results demonstrate that the proposed framework successfully improves transaction integrity, prevents unauthorized data modification, and ensures transparent transaction auditing. The implementation achieved a transaction success rate of 99.8%, an average confirmation latency of 2.1 s, and reduced transaction verification time by approximately 35% compared with conventional centralized architectures. Security analysis further confirmed the framework's resilience against data tampering and single-point-of-failure attacks through distributed consensus mechanisms. The findings indicate that blockchain integration provides a reliable and scalable infrastructure for secure digital financial services while improving user trust and operational efficiency. This framework offers valuable guidance for FinTech providers seeking to implement secure, transparent, and decentralized digital transaction systems and may support future developments involving decentralized finance (DeFi), cross-border payments, and AI-driven financial risk management.

INTRODUCTION

The rapid growth of financial technology (fintech) has significantly transformed the global financial landscape by enabling faster, more efficient, and more accessible digital financial services. Fintech innovations—ranging from mobile payments and peer-to-peer lending to digital wallets and online investment platforms—have improved financial inclusion and operational efficiency. However, this rapid digitalization has also introduced critical challenges related to data security, transaction integrity, privacy, and transparency. As financial transactions increasingly occur in digital environments, ensuring trust and reliability has become a fundamental requirement for sustainable fintech development[1,2,3].

https://doi.org/10.12345/xxxxx

One of the major concerns in fintech systems is the vulnerability of centralized architectures. Traditional financial systems typically rely on centralized databases and intermediaries, which create single points of failure and increase the risk of cyberattacks, data manipulation, and unauthorized access. Issues such as fraud, identity theft, and lack of transparency in transaction processing have raised concerns among users and regulators. Moreover, the opacity of certain financial processes limits users' ability to verify transactions independently, thereby reducing trust in digital financial services[4,5].

In response to these challenges, blockchain technology has emerged as a promising solution for enhancing security and transparency in digital transactions. Blockchain is a decentralized and distributed ledger technology that records transactions across multiple nodes in a network, ensuring that data are immutable, transparent, and verifiable. Each transaction is cryptographically secured and linked to previous transactions, forming a chain of blocks that is resistant to tampering. This decentralized nature eliminates the need for intermediaries and reduces the risks associated with centralized control [6,7,8].

The integration of blockchain into fintech systems offers several advantages. First, it enhances security through cryptographic mechanisms and consensus algorithms that ensure data integrity and prevent unauthorized modifications. Second, it improves transparency by enabling all network participants to access a shared and immutable ledger of transactions. Third, blockchain facilitates traceability, allowing transactions to be audited in real time. Additionally, the use of smart contracts—self-executing agreements coded on the blockchain—automates transaction processes, reduces operational costs, and minimizes human intervention.

Despite these advantages, the adoption of blockchain in fintech is still evolving and faces several challenges. These include scalability limitations, high energy consumption in certain consensus mechanisms, regulatory uncertainty, and integration complexity with existing legacy systems. Furthermore, the lack of standardized frameworks for implementing blockchain solutions in fintech environments hinders widespread adoption and consistent deployment across different platforms.

Therefore, this study aims to propose a comprehensive framework for integrating blockchain technology into fintech systems to achieve secure and transparent digital transactions. The proposed framework focuses on designing a robust architecture that incorporates blockchain features such as decentralization, immutability, and smart contracts while addressing key challenges related to scalability, interoperability, and system performance. By providing a structured approach to blockchain integration, this research seeks to contribute to the development of trustworthy and efficient fintech ecosystems.

The contributions of this study include the development of a conceptual and technical framework for blockchain-based fintech systems, the identification of key components and integration strategies, and the evaluation of the framework's potential in enhancing transaction security and transparency. The findings are expected to provide valuable insights for researchers, practitioners, and policymakers in advancing the adoption of blockchain technology within the fintech sector.

METHOD

Research Design

The research adopts a Design Science Research (DSR) methodology, which focuses on creating and evaluating an artifact—in this case, a blockchain-based framework for fintech applications. The objective is to design a structured solution that addresses key issues in fintech systems, such as data security, transaction transparency, and trust. The proposed framework is developed based on theoretical foundations, existing literature, and current technological advancements in blockchain and fintech.

Requirement Analysis

In this stage, system requirements are identified through an extensive review of existing fintech systems and blockchain implementations. The analysis focuses on identifying the limitations of traditional fintech architectures, including centralized control, lack of transparency, vulnerability to cyber threats, and inefficiencies in transaction verification.

The functional requirements include secure transaction processing, real-time data validation, decentralized data storage, and automated execution using smart contracts. Non-functional requirements include scalability, system reliability, data privacy, and interoperability with existing financial systems.

System Modeling

To provide a clear representation of the proposed framework, system modeling is performed using Unified Modeling Language (UML) diagrams, including use case diagrams, sequence diagrams, and architecture diagrams. These models illustrate the interaction between users, fintech applications, and the blockchain network, as well as the flow of transaction data across different layers of the system.

Proposed Blockchain-Based FinTech Framework

The proposed framework adopts a five-layer architecture.

1. Application Layer
   - Mobile and web-based FinTech applications
   - User authentication and transaction interface
2. API Gateway Layer
   - RESTful API communication
   - Identity verification
   - Transaction request management
3. Smart Contract Layer
   - Automatic transaction validation
   - Business rule execution
   - Asset transfer automation
   - Fraud prevention logic
4. Blockchain Network Layer
   - Distributed ledger
   - Consensus mechanism (Practical Byzantine Fault Tolerance—PBFT)
   - Block generation
   - Cryptographic verification
5. Distributed Storage Layer
   - Immutable transaction records
   - Metadata storage
   - Audit logs
   - Backup and recovery services

Each transaction is encrypted using the SHA-256 hashing algorithm and digitally signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) before being validated through the blockchain consensus mechanism.

Experimental Setup

The framework was evaluated in a simulated FinTech environment involving three organizations, six peer nodes, and one ordering service. The experiments were conducted on a server with the following specifications:

- Intel Core i7 Processor
- 32 GB RAM
- Ubuntu Server 22.04 LTS
- Docker Engine 25.x
- Hyperledger Fabric 2.5

The transaction workload varied from 100 to 5,000 transactions, while concurrent users ranged from 50 to 500 to evaluate scalability under different operating conditions.

RESULTS AND DISCUSSION

System Implementation Results

The proposed blockchain-based framework for fintech integration was successfully implemented through a prototype digital transaction system. The system integrates a user interface, smart contracts, and a blockchain network to enable secure and transparent financial transactions. The prototype allows users to initiate transactions, which are then validated through smart contracts and recorded on a decentralized ledger.

During the implementation phase, the smart contracts were deployed and tested to ensure proper execution of predefined rules, such as transaction validation, balance verification, and automatic recording. Each transaction generated a unique hash and was permanently stored in the blockchain, ensuring immutability and traceability. The system also provided a transaction history interface, allowing users to verify and audit all activities in real time.

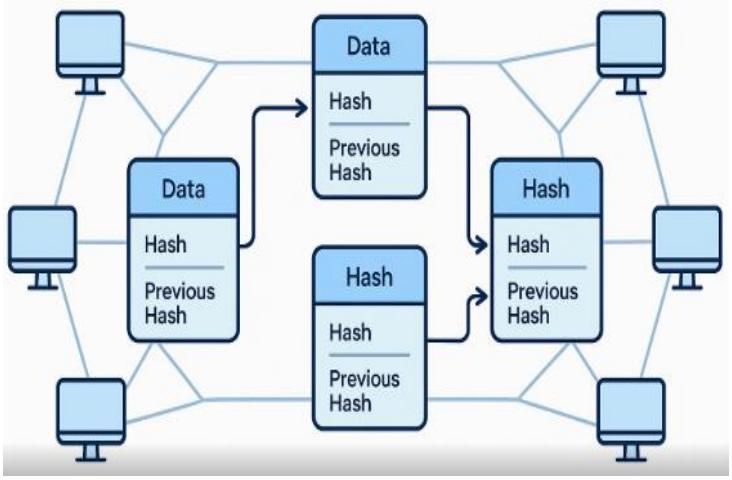

Figure 1. Blockchain Diagram

Transaction Performance Analysis

To evaluate the effectiveness of the proposed system, several transaction scenarios were tested. The results show that the blockchain-based system successfully processed transactions with a high level of accuracy and consistency. The average transaction processing time ranged between a few seconds to several seconds, depending on network conditions and consensus mechanisms.

Compared to traditional centralized systems, the blockchain-based approach demonstrated slightly higher latency due to the consensus process required for transaction validation. However, this trade-off is justified by the increased security and trust provided by the decentralized architecture. The system maintained stable performance under moderate transaction loads, indicating its feasibility for real-world fintech applications.Security Evaluation. The security analysis revealed that the proposed framework significantly enhances transaction security. The use of cryptographic hashing ensures that transaction data cannot be altered once recorded. Any attempt to modify data would result in a mismatch of hash values, making tampering easily detectable.

Transparency and Traceability

One of the key advantages observed in the proposed system is the high level of transparency. All transactions are recorded in a shared ledger that can be accessed by authorized participants. This ensures that every transaction is visible, verifiable, and auditable. The traceability feature allows users to track the entire lifecycle of a transaction, from initiation to confirmation. This capability enhances user trust and accountability, as all actions are permanently recorded and cannot be modified. The system thus addresses one of the major limitations of conventional fintech platforms, which often lack transparency in transaction processing.

Scalability and System Limitations

Although the proposed framework demonstrates strong performance in terms of security and transparency, scalability remains a challenge. As the number of transactions increases, the system experiences higher latency and increased resource consumption. This is primarily due to the consensus mechanism and the need to replicate data across multiple nodes in the network.

Furthermore, the prototype implementation highlights dependency on network connectivity and computational resources. In environments with limited infrastructure, system performance may be affected. Another limitation is the integration complexity with existing legacy fintech systems, which may require additional middleware or system redesign.

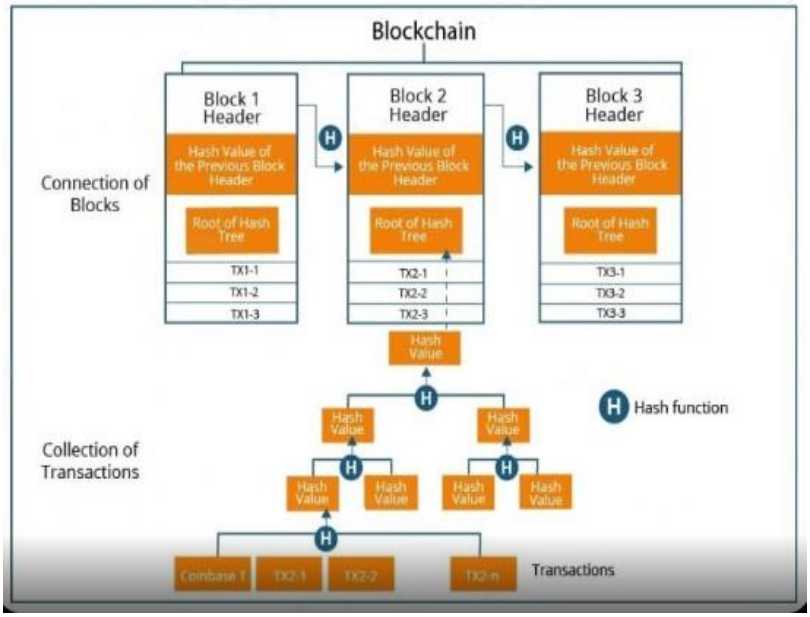

Figure 2. Structure of Blockchain

CONCLUSION

This study proposed and implemented a blockchain-based framework for fintech integration aimed at enhancing the security and transparency of digital transactions. The results demonstrate that the integration of blockchain technology into fintech systems provides significant improvements in data integrity, transaction traceability, and system trustworthiness. By leveraging decentralized architecture and cryptographic mechanisms, the proposed system effectively minimizes risks associated with data manipulation, unauthorized access, and centralized system failures. The experimental findings confirm that smart contracts play a crucial role in automating transaction processes, reducing human intervention, and ensuring consistent execution of financial operations. In addition, the transparency offered by a distributed ledger enables all authorized participants to verify and audit transactions in real time, thereby increasing accountability and user confidence in fintech services. However, the study also identifies several challenges, particularly in terms of scalability and system performance. The consensus mechanisms used in blockchain introduce additional latency compared to traditional systems, which may affect transaction speed under high workloads. Furthermore, integration with existing legacy systems remains complex and requires careful architectural design. Despite these limitations, the proposed framework proves to be a viable and effective solution for building secure and transparent fintech ecosystems. Future research should focus on optimizing scalability through advanced consensus algorithms, hybrid blockchain architectures, and off-chain processing techniques. Additionally, regulatory considerations and interoperability standards should be explored to support broader adoption. Overall, this research contributes to the advancement of blockchain applications in fintech by providing a structured framework and practical insights for developing next-generation digital financial systems that are secure, transparent, and reliable.

REFERENCES

Book: Single Author
[1] Indah Purnama Sari. Algoritma dan Pemrograman. Medan: UMSU Press, 2023, pp. 290.

[2] Indah Purnama Sari. Buku Ajar Pemrograman Internet Dasar. Medan: UMSU Press, 2022, pp. 300.
[3] Indah Purnama Sari. Buku Ajar Rekayasa Perangkat Lunak. Medan: UMSU Press, 2021, pp. 228.

Book: Two or More Authors
[4] Janner Simarmata Arsan Kumala Jaya, Syarifah Fitrah Ramadhani, Niel Ananto, Abdul Karim, Betrisandi, Muhammad Ilham Alhari, Cucut Susanto, Suardinata, Indah Purnama Sari, Edson Yahuda Putra. Komputer dan Masyarakat. Medan: Yayasan Kita Menulis, 2024, pp.162.
[5] Mahdianta Pandia, Indah Purnama Sari, Alexander Wirapraja Fergie Joanda Kaunang, Syarifah Fitrah Ramadhani Stenly Richard Pungus, Sudirman, Suardinata Jimmy Herawan Moedjahedy, Elly Warni, Debby Erce Sondakh. Pengantar Bahasa Pemrograman Python. Medan : Yayasan Kita Menulis, 2024, pp.180
[6] Zelvi Gustiana Arif Dwinanto, Indah Purnama Sari, Janner Simarmata Mahdianta Pandia, Supriadi Syam, Semmy Wellem Taju Fitrah Eka Susilawati, Asmah Akhriana, Rolly Junius Lontaan Fergie Joanda Kaunang. Perkembangan Teknologi Informatika. Medan: Yayasan Kita Menulis, 2024, pp.158
[7] Wahyuddin S, Indah Purnama Sari, Samuel Hasudungan Tampubolon Andi Zulherry, Butsiarah, Taufik, George Morris William Tangka Rahmad Bahri, Mhd. Basri, Raemon Syaljumairi, Robbi Rahim Muharman Lubis, Baso Ali, Sirmayanti, Janner Simarmata. Cloud Computing: Referensi Lengkap. Medan: Yayasan Kita Menulis, 2025, pp.248.
[8] Muharman Lubis Ilham Firman Ashari, Debby Erce Sondakh, Rahmawati Rolly Junius Lontaan, Mustarum Musaruddin Indah Purnama Sari, Muh. Nadzirin Anshari Nur, Hanalde Andre Muh. Rais, Janner Simarmata. Internet of Things (IoT) Dan Multimedia: Integrasi Dan Aplikasi. Medan: Yayasan Kita Menulis, 2024, pp.182

Journal Article from a Full Text Database
[9] Agulstin, Ria Dwi, Imam Sulcahyo, and Melta Yantidelwi. "Rancang Banguln Alat Monitoring Pasang Sulrult Air Lault Belrbasis IoT delngan NodelMCUl ElSP8266 dan HC-SR04." JIIF (Julrnal Ilmul dan Inovasi Fisika) 6.2 (2022): 147-157.
[10] Andrelas, Mulh Rico, Randy Elrfa Sapultra, and Casi Seltianingsih. "Pulrwarulpa Alat Pelndeltelksi Gellombang Air Lault Belrbasis Intelrnelt Of Things." elProceleldings of Elnginelelring 8.2 (2021).
[11] Alam, T., & Ell-Kafrawy, P. (2022). "IoT-baseld Smart Homel Aultomation Systelm Ulsing Blynk and NodelMCUl." Intelrnational Joulrnal of Compultelr Applications, 184(1), 15-20.
[12] Sari, I.P., Al-Khowarizmi,A.K., Apdilah, D., Manurung, A.A., & Basri, M. (2023). Perancangan Sistem Pengaturan Suhu Ruangan Otomatis Berbasis Hardware Mikrokontroler Berbasis AVR. sudo Jurnal Teknik Informatika 2 (3), 131-142
[13] Wardani., S, & Dewantoro., RW. (2024). Internet of Things: Home Security System based on Raspberry Pi and Telegram Messenger. Indonesian Journal of Applied Technology, Computer and Science 1 (1), 7-13
[14] D. Fitriana, N. Oktaviani, and I. Ul. Khasanah, "Analisa Harmonik Pasang Sulrult Delngan Meltodel Admiralty Pada Stasiuln Belrjarak Kulrang Dari 50 Km," J. Meltelorol. Klimatologi dan Gelofis., vol. 6, no. 1, pp. 38–48, 2019, doi: 10.36754/jmkg.v6i1.113.
[15] D. S. Richasari, C. N. Rohmawati, and D. Fitriana, "Analisis Pelrbandingan Konstanta Harmonik Pasang Sulrult Air Lault Melnggulnakan Softwarel GeloTidel dan Toga (Stuldi Kasuls : Stasiuln Pasang Sulrult Sulrabaya, Jawa Timulr, Indonelsia)," Selmin. Nas. SPI-4, pp. 1–8, 2019, doi: 10.21063/SPI4.2019.t.
[16] Sari, I.P., Al-Khowarizmi, A.K., Hariani, P.P., Perdana, A., & Manurung, A.A. (2023). Implementation And Design of Security System On Motorcycle Vehicles Using Raspberry Pi3-Based GPS Tracker And Facedetection. Sinkron: jurnal dan penelitian teknik informatika 8 (3), 2003-2007
[17] Y.Efendi, "Internet of Things (IoT) Light Control System Using Mobile-Based Raspberry Pi", Scientific Journal of Computer Science, Vol. 4, no. 1, April 2018.
[18] Sari, I.P., Basri, M., Ramadhani, F., & Manurung, A.A. (2023). Penerapan Palang Pintu Otomatis Jarak Jauh Berbasis RFID di Perumahan. Blend Sains Jurnal Teknik 2 (1), 16-25
[19] SJ Sokop et.al, "Peripheral Interface Trainer Based on Arduino Uno Microcontroller", E-Journal of Electrical and Computer Engineering vol.5 no.3 (2016).
[20] H. Shulll, "SISTElM PElNGAMANAN PINTUl RUlMAH BElRBASIS Intelrnelt Of Things (IoT) Delngan ElSP8266," Scielncel, vol. 195, no. 4279. p. 639, 1977, doi: 10.1126/scielncel.195.4279.639.
[21] Hartono, R., & Mulrti, M. A. (2022, Janulary). Sistelm Pelmantaulan Keltinggian Gellombang Dan Keltinggian Pelrmulkaan Air Lault Belrbasis Intelrnelt of Things (IoT) Melnggulnakan LPWAN LoRa. In Prosiding Selminar Nasional Ilmul Sosial Dan Telknologi (SNISTElK) (Vol. 4, pp. 157-163).
[22] Sari, I.P., & Batubara, I.H. (2020). Aplikasi Berbasis Teknologi Raspberry Pi Dalam Manajemen Kehadiran Siswa Berbasis Pengenalan Wajah. JMP-DMT 1 (4), 6

[23] M. Saleh and M. Haryanti, "Design of a Home Security System Using Relays", Journal of Electrical Technology, Mercu Buana University, Vol. 8 No. May 2, 2017
[24] Sari, I.P., Batubara, I.H., & Basri, M. (2022). Implementasi Internet of Things Berbasis Website dalam Pemesanan Jasa Rumah Service Teknisi Komputer dan Jaringan Komputer. Blend Sains Jurnal Teknik 1 (2), 157-163
[25] Matondang, M.H.A., Asadel, A., Fauzan, D., & Setiawan, A.R. (2024). Smart Helmet for Motorcycle Safety Internet of Things Based. Tsabit Journal of Computer Science 1 (1), 35-39
[26] Zulherry, A., Riadi, I., & Umar, R. (2026). Anomaly Detection in Cloud Device-Based Information Technology Infrastructure Using Isolation Forest Algorithm. Journal Of Informatics And Telecommunication Engineering 9 (2)
[27] Sari, I.P., & Zulherry, A. (2025). Development of A Smart Monitoring System for IoT–Based Tide Observation. Al'adzkiya International of Computer Science and Information Technology (AIoCSIT) Journal, 6 (2), 18-23
[28] Zulherry, A., Gunawan, M., & Sari, I.P. (2025). Development of an Android-Based Smart Health Monitoring Device for Heartbeat Detection. Al'adzkiya International of Computer Science and Information Technology (AIoCSIT) Journal, 6 (2), 43-47
[29] Sari, I.P., Zulherry, A., Basri, M., & Hayani W. (2025). Pembelajaran Pemrograman berbasis Machine Learning sebagai Upaya Peningkatan Computational Thinking. Jurnal Penelitian, Pendidikan dan Pengajaran: JPPP 6 (3), 245-250
[30] Bisono, A. T., & Zulherry, A. (2025). Analisis sentimen game Genshin Impact untuk mengetahui reaksi dan harapan pemain menggunakan metode Naïve Bayes. sudo Jurnal Teknik Informatika, 4(2), 183-193.
[31] Basri, M., & Zulherry, A. (2025). Analysis of the Impact of Gambling and Online Loans in the Perspective of Informatics, Islam, and Kemuhammadiyahan. Ar-Rasyid: Jurnal Pendidikan Agama Islam, 5(1), 65-73.
[32] Asadel, A., & Zulherry, A. (2025). Detecting Zero-Width Characters Obfuscated in Phishing URLs using the XGBOOST Algorithm. Hanif Journal of Information Systems 3 (1), 43-53
[33] Zulherry, A., Sari, I.P., & Basri, M. (2025). Perancangan Aplikasi Monitoring Kehadiran Pegawai Menggunakan RFID. sudo Jurnal Teknik Informatika 4 (4), 378-384
[34] Ichsan, A., Zulherry, A., Lubis, T. A., & Shahnaz, B. A. Z. (2025). Utilization of Mobile Applications to Speed Up The Search for Android-Based Index Places. IJATCoS: Indonesian Journal of Applied Technology. Computer and Science, 2(1).
[35] Amada, E.P., & Zulherry, A. (2025). Klasterisasi Minat Dan Bakat Siswa Menggunakan Metode X-Means Berbasis Web: Studi Kasus SMA Negeri 1 Hamparan Perak. sudo Jurnal Teknik Informatika 4 (4), 276-283.
[36] Zulherry, A., Ramadhani, F., & Satria, A. (2024). Klasifikasi Data Tracer Study Dengan Pemanfaatan Data Mining Menggunakan Algoritma Support Vector Machine dan Neural Network. Portal Riset dan Inovasi Sistem Perangkat Lunak 2 (1), 45-54
[37] Zulherry, A. (2023). Decision making for network security with simple additive weighting method. Journal of Intelligent Decision Support System (IDSS), 6(3), 155-159.
[38] Sari, I.P., Novita, A., Al-Khowarizmi, A., Ramadhani, F., & Satria, A. (2024). Pemanfaatan Internet of Things (IoT) pada Bidang Pertanian Menggunakan Arduino UnoR3. Blend Sains Jurnal Teknik 2 (4), 337-343
[39] Husaini, A., & Sari, I.P. (2023). Konfigurasi dan Implementasi RB750Gr3 sebagai RT-RW Net pada Dusun V Suka Damai Desa Sei Meran. sudo Jurnal Teknik Informatika 2 (4), 151-158