DOI: https://doi.org/10.53486/ser2025.29
International Scientific and Practical Conference,
4th Edition, March 27-28, 2025, Chișinău, Moldova

ENHANCING DIGITAL SECURITY IN THE FINANCIAL SECTOR WITH AI, IOT, AND BLOCKCHAIN

Zoran CEKEREVAC
Independent Researcher, Belgrade, SERBIA
ORCID: 0000-0003-2972-2472
Lyudmila PRIGODA
Maykop State Technological University
Maykop, RUSSIAN FEDERATION
ORCID: 0000-0002-4762-3892

Petar ČEKEREVAC
Independent Researcher, Belgrade, SERBIA
ORCID: 0000-0001-6100-5938

Abstract: *Integration of Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain technology represents a significant step towards enhancing digital security in the financial sector. AI enables the identification of suspicious behavior patterns by real-time analysis of large amounts of data, thereby improving fraud detection and automating threat response. Based on historical data, the AI's predictive analytics assist in forecasting potential threats and enhancing proactive security measures. IoT devices gather real-time data, enabling financial institutions to swiftly respond to changes and make informed decisions while at the same time enhancing transaction security by monitoring network activities and recognizing suspicious patterns. Blockchain technology provides data integrity and transparency through decentralized ledgers, reducing the likelihood of fraud and increasing resilience to cyber-attacks. Smart contracts automate transactions, minimizing the risk of human error and fraud. By combining these technologies, financial institutions establish a robust framework for protecting their systems and processes, reducing the risk of fraud and cyber-attacks, and increasing user's trust. Security measures such as encryption, authentication, and regular software updates further ensure the safety of IoT devices and blockchain networks, thereby strengthening the overall digital security infrastructure in the financial sector. In this paper, the authors analyze the potential of each of these technologies and the synergy of their integration.*

Keywords: *Artificial Intelligence (AI), Internet of Things (IoT), Blockchain, Digital Security, Financial Sector, Decentralization, Smart Contracts.*

UDC: *[004.056:336]:004.8*

Classification JEL: *G21, G32, G34, G38, K24, L86, O33, O38*

1. Introduction

General Introduction

Digital transformation has facilitated faster and more efficient information exchange but opened the door to new threats and risks. In today's globally connected digitalized world, digital security has become crucial in protecting data, resources, and privacy. Therefore, digital security has become imperative for all organizations, from small and medium-sized enterprises (SMEs) to large corporations, banks, and state financial institutions.

The level of protection largely depends on the size, significance, and levels of the protection knowledge of those who need to be protected. Large companies can afford complex infrastructures and teams of experts. SMEs have fewer resources and cannot invest in advanced security systems. This resource disparity makes SMEs more vulnerable to cyber-attacks, which can have significant economic and reputational consequences.

They frequently can apply only basic security measures that prove inadequate against advanced attacks [1].

Banks and government financial institutions hold valuable information and economic assets, and they are among the most attractive targets for cybercriminals. Such entities must maintain high-security standards to combat increasingly sophisticated threats, including phishing attacks, ransomware, and network infrastructure attacks. Successful implementation of digital security in the banking sector is crucial for maintaining client trust and financial stability.

The levels of digitalization vary worldwide. That affects different regions' ability to overcome cyber threats. Developed countries have advanced digital infrastructure and sophisticated security protocols, but many developing countries struggle with fundamental digitalization problems. That includes internet access and cybersecurity. This disparity can lead to uneven levels of protection, spillover risks from region to region, and increased global vulnerability.

Objective

This paper aims to present the capabilities of AI, IoT, and blockchain technologies and the synergistic effects of their integration that can significantly improve digital security through more effective threat detection, secure data storage, and better protection of network activities. That is significant because these technologies represent the future of digital security and can transform how we combat cyber threats. Additionally, the paper examines benefits such as enhanced proactive security and reduced risks. It also addresses potential challenges related to the implementation of these technologies. This paper enhances comprehension of how integrating these technologies can improve digital security in the financial sector by reviewing existing research and new findings.

2. Methodology

The authors prepared this paper using research methods commonly employed in review articles. These methods include searching, selecting, analyzing, and synthesizing literature. The literature review involved searching databases such as Google Scholar, IEEE Xplore, SpringerLink, and MDPI. Due to the specificities related to the topic, we also searched relevant websites that deal with information system security issues. Keywords such as "quantum cryptography," "digital security," and "critical evaluation" were used. Papers were included based on relevance, quality, and publication in the last eight years. The authors included some of their previous papers about IoT, blockchain technology, and digital security. The collected papers were critically reviewed and analyzed using methodological standards such as the validity and reliability of sources and the significance of findings for the current topic. The authors organized and synthesized collected information using thematic analysis. They identified key themes and patterns and created a conceptual framework integrating existing knowledge. To reduce the length of the article, we often utilized bullet text. Based on the analysis, we identified existing gaps in the literature and proposed directions for future research in digital security.

Research Question and Hypotheses

The authors based their research on the following research question and hypotheses:

- *Research Question:* How does the integration of Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain technology impact the enhancement of digital security in the financial sector?

- *Null Hypothesis (H_0):* The integration of AI, IoT, and blockchain technology does not significantly affect the enhancement of digital security in the financial sector.
- *Alternative Hypothesis (H_1):* The integration of AI, IoT, and blockchain technology significantly improves digital security in the financial sector by enhancing fraud detection, automating threat responses, and ensuring data integrity.

3. Technological Innovations in Digital Security

Technological innovations in digital security are crucial in today's digitalized world. They play a key role in protecting data and systems. With the increase in threats, developing new technologies and strategies is becoming more significant. These innovations help to combat threats and enable organizations to enhance their security postures and protect resources efficiently. Although numerous and necessary, innovations are not accessible to everyone. The larger and more significant the organization is, the more interested it is in quickly adopting each innovation to increase security, as potential attackers also closely monitor innovations for opposite purposes. Financial institutions are always among the first adopters of all technological innovations to improve digital security, as potential attackers watch innovations closely to stay ahead. It is a continuous race. Some of modern, key innovations include:

1. *Artificial Intelligence (AI) and Machine Learning:* They can independently or within software packages process large datasets and identify patterns that suggest potential threats.
2. *Blockchain Technology:* This technology is well-known for its application in cryptocurrencies, but its security application is much broader [2]. It allows decentralized and secure transaction recording, reducing the risk of data manipulation.
3. *Cryptography:* Cryptography ensures that data is inaccessible to unauthorized users. Advanced cryptographic algorithms have become a standard practice for data protection during transactions. One of the advanced innovations is quantum cryptography, which uses principles of quantum physics to create unbreakable encryption systems. Quantum key distribution allows secure transmission of encryption keys, and any eavesdropping attempts are immediately detected. [3]
4. *Biometric Authentication*: It uses physical characteristics such as fingerprints, facial recognition, or iris scanning to verify user identities and provide additional protection for user accounts. These methods are more secure than traditional passwords, as they are unique to each individual and highly resistant to misuse, providing a high level of security. Biometric authentication is increasingly used in smartphones, banking applications, and access control systems.
5. *Zero Trust Architecture:* This security approach assumes that no user, person, or device, whether inside or outside the organization's network, can be trusted automatically. This approach requires constant verification of each user and device before granting access to resources. The Zero Trust model uses techniques such as multi-factor authentication, micro-segmentation, and

continuous monitoring of activities to ensure security [4] It is increasingly used in various industries, most notably at airports.

6. *Cloud Security:* The banking sector increasingly relies on cloud computing to enhance scalability and efficiency. This technology allows centralized data protection and better resource management [5]. As more organizations move to the cloud, cloud security becomes crucial. Cloud service providers employ advanced security measures such as data encryption in transit and at rest, as well as role-based access control. Additionally, cloud security tools allow organizations to monitor activities and identify threats in real time [6].
7. *Internet of Things (IoT) Security:* With the growing use of IoT devices, their security becomes critical. IoT devices often have limited protection capabilities, making them vulnerable to attacks [7] Innovations in IoT security include improved device authentication, communication encryption, and proactive monitoring of network activities to detect and neutralize threats.
8. *Behavioral Analytics:* It uses user behavior data to identify suspicious activities. For example, if the system recognizes unusual patterns in system usage (such as accessing sensitive data at unusual times), it can automatically trigger security checks. This technology helps to identify internal threats and insider attacks. [8]
9. *Secure Access Service Edge (SASE):* This architecture combines network security and optimization capabilities into a single platform. This technology allows organizations to provide secure access to resources regardless of user location. SASE includes functions such as secure internet access, private cloud networks, and threat protection [9]
10. *Identity and Access Management (IAM):* These technologies enable organizations to manage user identities and access control. This includes user authentication methods, permission management, and access tracking. IAM tools ensure that only authorized users have access to sensitive information. [10]
11. *Automated Systems:* They use algorithms to monitor network activities and detect unknown or suspicious events. They enable rapid response to potential threats.
12. *Data Loss Prevention (DLP):* DLP enables monitoring and control of data to prevent unauthorized use. These systems can detect and block data attempting to be transferred outside closed networks.

As can be seen, innovations are numerous and diverse. However, each of these innovations brings uncertainties regarding their reliability and resilience to attacks. Comprehensive verification requires resources and time, both of which are limited due to the rapid pace of digitalization processes.

4. AI, IoT, and Blockchain Technologies for Digital Security

Artificial Intelligence (AI)

AI is one of the most mentioned terms in modern communications, perceived as a technology that enables computers and machines to perform tasks that would otherwise require human intelligence, and perform these tasks in the same way humans would. It plays a crucial role in enhancing digital security, especially in the context of banks and state institutions, but also on the side of malicious attackers. Using machine learning algorithms, AI systems can analyze vast amounts of data to detect threats and anomalies in real-time. From the perspective of AI's positive impact on security, the following points stand out [11, 12]:

- *Threat Detection:* AI can quickly, in real-time analyze vast amounts of data and identify suspicious activities, such as unknown accesses or unusual usage

DOI: https://doi.org/10.53486/ser2025.29
International Scientific and Practical Conference,
4th Edition, March 27-28, 2025, Chișinău, Moldova

patterns. AI can detect anomalies in network traffic that might indicate hacking attempts. Machine learning can help detect and block malware before it causes damage [13].

- *Identity Management:* AI enables precise management of user identities and access control, which is crucial for accessing sensitive information.
- *Automation of Security Checks:* AI can automate security checks and responses to security incidents, reducing reaction time and increasing the efficiency of security teams.
- From the perspective of threats to users, the following risks stand out:
- *Malicious attackers* can use AI to create sophisticated attack methods, such as phishing campaigns, attack software that adapts, and deep-fake technologies.
- *Privacy and Data Security:* Using AI to analyze data can compromise confidentiality and security, especially if appropriate protection measures are not used.
- *Ethical Issues:* The application of AI in security also raises ethical questions, such as transparency and accountability in AI-based decision-making.

Artificial intelligence can be a powerful tool for improving digital security, but it also represents a new dimension of risk that requires careful management and constant improvement of defense strategies. Therefore, when analyzing AI application possibilities, it is always essential to consider the most unfavorable scenarios. Table 1 presents a comprehensive framework for understanding defensive and offensive artificial intelligence.

Table 1. Prevalence of AI in Digital Security

Type of AI in Cybersecurity	Goal	Examples
Defensive AI	Leverages AI techniques to protect computer systems and networks from attack	Anti-malware; Intrusion detection systems (IDS)
Offensive AI	Deploys AI techniques to attack computer systems and networks	Developing new cyberattacks. Automating the exploitation of existing vulnerabilities
Adversarial AI	Maliciously exploits and/or attacks AI/ML systems and data	Poisoning training data; Manipulating input data

Source: Malatji, M., Tolah, A. [12]

Analyses of offensive AI cyber-attacks reveal their complex and dynamic nature. Accordingly, adaptive defensive mechanisms, also supported by artificial intelligence, are necessary. Each AI-driven attack is multidimensional and encompasses many implications, strategies, motivations, and social impacts. This makes protection challenging and underscores the need for even more sophisticated defense methods.

Internet of Things (IoT) and Its Impact on Financial Operations

The Internet of Things (IoT), a set of technologies that connect and exchange data via the Internet or other networks, is becoming increasingly significant in the economy. IoT enables real-time data collection and exchange, which is crucial for financial transactions. It helps analyze clients' assets and digitalize the operations of financial companies, improving services and customer experience. IoT supports data transmission across various devices connected via Bluetooth, WiFi, or USB. IoT devices also allow monitoring of network activities and threat detection, enhancing digital security. Ensuring their security is crucial because of their network connectivity and commonly inadequate security protocols, which make them frequent targets for attacks.

The global IoT market in the BFSI sector reached $2.03 billion by 2023, up from $249.4 million in 2018, with an annual growth rate of 52.1% [14].

How IoT Affects Financial Operations

The Internet of Things (IoT) has numerous applications in financial operations that can enhance efficiency, security, and quality of service. Some of the key applications are:

1. *Real-time Data Collection:* Real-time data collection facilitates quick analysis and decision-making based on information. For example, clients can be immediately notified when an unexpectedly large sum of money is spent. Smart devices in branches can monitor queues, enable appointment scheduling, and inform clients about waiting times. They can assist clients in finding the nearest branch. Branches can quickly share customer data for personalized services. By using data, banks can make key decisions to save money and optimize branch operations [15]
2. *Enhanced Security and Fraud Detection:* Financial companies invest in IoT to prevent potential fraud and protect user accounts. IoT promptly detects unusual behavior and controls account access, providing additional security. Analytics provide insights into the bank's website and mobile app use, helping quickly respond to suspicious activities and prevent fraudulent transactions [16]. IoT technology is integrated into biometric authentication.
3. *Process Automation:* IoT technology can automate various operations such as opening accounts, deactivating credit cards, processing client requests, reducing costs, and increasing efficiency. Automated data collection and analysis can speed up loan approval processes and other administrative tasks. [17]
4. *Improved Customer Service:* IoT enables financial institutions to gain deeper insights into client needs and offer tailored services. IoT devices collect data that enhances financial services throughout the customer lifecycle. Banks can send customized offers and reminders proactively and streamline tasks such as onboarding new users and resolving complaints. IoT provides real-time data to support teams, enabling informed decision-making. Data analytics help employees manage clients' money and develop valuable reports. [17]
5. *Intelligent Asset Tracking:* IoT enables real-time asset tracking, improving asset management and protection. Banks use IoT devices to track equipment, optimize usage and efficiency, and reduce costs. Collected data helps manage capacities, identify locations, and record performance, lowering costs and downtimes. IoT networks improve security and enable real-time data sharing, while equipment monitoring provides accurate information on the condition and performance of devices. [15]
6. *Market Data:* IoT enables better tracking and market data analysis, optimizing investments. Private investors and corporations use real-time data for informed decision-making. The analysis of collected data helps build profitable strategies and investment plans, as well as train autonomous trading systems [15]

DOI: https://doi.org/10.53486/ser2025.29
International Scientific and Practical Conference,
4th Edition, March 27-28, 2025, Chișinău, Moldova

7. *Inventory Management:* IoT automatically collects and analyzes data for inventory management. Smart collateral management allows banks to remotely monitor clients' assets, such as car, home, and equipment mortgages. Sensors monitor asset conditions and enable automatic issuance of repair loans or remote car disabling in case of non-payment. [15]
8. *Wireless Payments:* IoT enables wireless payments via devices like smartwatches and phones, transforming banking and providing users with access to funds anywhere, anytime. IoT devices facilitate payments and detect wearable devices within range, thereby enhancing the connection with clients. Data from wearable devices helps insurance companies calculate premiums based on health statistics. They are also used for contactless payments and account balance checks. [15]

Examples of IoT Applications in Financial Operations

Fintech, or financial technology, uses new technologies to enhance and automate financial services, enabling faster, more efficient, and secure transactions and services. Banking has been using the concept of the Internet of Things for decades. Numerous examples of IoT applications in financial operations include [15]:

- *Smart ATMs:* ATMs are examples of IoT devices that use technologies for improved security and functionality.
- *Wireless Payments and Transactions:* Payments via smartphones and smartwatches allow users to access their bank services remotely.
- *Mobile-based Point-of-Sales (mPOS) Systems:* Allow companies to accept payments via mobile devices such as smartphones and tablets, providing greater flexibility and mobility in sales operations.

There are also many other less noticeable but significant and widespread applications [14]:

- *Smart Devices for Financial Monitoring:* IoT devices automatically collect and analyze data on expenses, income, and users' financial status.
- *Smart Banking Machines:* Track user transactions and provide additional security measures.
- *Inventory Tracking:* IoT sensors monitor product levels and automatically notify managers about the need for restocking. [18]
- *Smart Security Alarms*: Detect unknown activity and automatically notify owners or the police [19].

Fintech also uses new technologies to improve and automate financial services, such as [17]:

1. Mobile Banking: Includes apps for banking transactions via smartphones, which enable financial management regardless of the bank and client locations.
2. *P2P (Peer-to-Peer) Lending:* Platforms connect lenders and borrowers directly, allowing lower interest rates and higher returns for users.
3. *Cryptocurrencies:* Digital currencies like Bitcoin and Ethereum use blockchain technology for secure and decentralized transactions.
4. *Robo-Advisors:* Automated systems for investment advice and portfolio management, financial planning, and automated transactions. They offer affordable, personalized, and adaptable investment services.

5. *Payments:* Digital or e-wallet, a software application or online service that allows users to store and manage their financial information and funds electronically.
6. *Insurance (Insurtech):* Technologies to improve processes, reduce costs in the insurance sector, and adjust premiums.

Fintech is transforming the way financial operations are conducted, making them more accessible, transparent, and efficient. IoT technology has revolutionized financial operations, enabling financial institutions to provide faster, more secure, and personalized services to their clients [17].

Can IoT Be a Victim of Attacks?

All electronic data can be targeted, no matter where it is located. It is easier to attack data that is somehow connected to the Internet [20]. The Internet of Things (IoT) devices can be compromised by attacks that may be transferred to the associated blockchain. Hence, financial IoT devices and networks can be exposed to various types of attacks, including [21, 22, 23]:

1. *Unauthorized Device Access:* Attackers exploit weaknesses in device passwords or firmware to gain unauthorized access, allowing them to manipulate device functionalities or infiltrate the network.
2. *Man-in-the-Middle (MitM) Attacks:* Attackers intercept communication between devices and servers, injecting malicious content, stealing data, or manipulating information. Targeting financial IoT devices, MitM attacks can be especially hazardous as they may enable attackers to steal sensitive information, including financial transactions or authentication details [24].
3. *Denial of Service (DoS) Attacks:* Attackers use botnets to flood services with requests, which can lead to service disruption or downtime.
4. *Firmware Hijacking:* Attackers install malicious software on the device if the firmware is poorly maintained, taking control of the device.
5. *Physical Attacks:* Attackers physically access devices and implant malicious code via USB devices or other physical methods.
6. *Encryption Attacks:* Attackers can decrypt encrypted data if they can access encryption keys, stealing sensitive information.
7. *Credential Attacks:* Attackers exploit password weaknesses, such as default passwords, to gain unauthorized access to devices.
8. *Side-Channel Attacks:* Attackers use power consumption or sound to gain information about encrypted data.
9. *Brute Force Password Attacks:* Attackers use brute force methods to try all possible password combinations until they find the correct one.
10. *Update Vulnerability Exploits:* Attackers exploit weaknesses in software updates or the lack of them, which can allow unauthorized access or control of the device.

These attacks require careful defense management and continuous improvement of strategies to ensure the security of financial IoT devices and networks.

Blockchain Technology

The intangible assets, such as licenses, trademarks, patents, and cryptocurrencies, are not new in the financial sector. Blockchain, known thanks to Bitcoin, enables decentralized and transparent data protection, ensuring data integrity and authenticity. It is ideal for secure storage and verification of transactions, reducing the risk of fraud and data manipulation [25].

DOI: https://doi.org/10.53486/ser2025.29
International Scientific and Practical Conference,
4th Edition, March 27-28, 2025, Chișinău, Moldova

Blockchain plays a significant role in finance, allowing transactions without time constraints and independent of banks and states. Improvements in hardware and communications speed up transactions, while increased market capitalization stabilizes the value of cryptocurrencies. Blockchain reduces transaction costs by eliminating intermediaries and reducing administrative efforts [26]

Blockchain technology is resistant to many types of attacks, including MITM attacks. However, IoT devices connected to the blockchain can be compromised if not properly secured. That can impact the blockchain. It can happen because of:

- *Compromised data.* Compromised IoT devices can send compromised data to the blockchain. That undermines data integrity.
- *Smart contract attacks.* Attackers can manipulate smart contracts on the blockchain if they gain control of the IoT device.
- *Distributed Denial of Service (DDoS) Attacks:* Compromised IoT devices can be used for DDoS attacks, overwhelming the network.
- *Identity Theft and Authentication:* Attackers can take control of IoT device identifiers and authentication data, gaining unauthorized access to the blockchain.
- *Ransomware Attacks:* Attackers can lock IoT device data and demand ransom, complicating the situation.

Due to these risks, it is essential to implement robust security measures to protect IoT devices and networks, as well as effective strategies to ensure the integrity and security of blockchain systems.

Attacks can be prevented or mitigated by implementing the following protective measures:

1. *Pre-blockchain Communication Security:* Well-secured communication between IoT devices and the blockchain network makes it difficult for attackers to manipulate data before it reaches the blockchain.
2. *Using Encryption:* Strong encryption methods for communication between IoT devices and the blockchain network reduce the risk of MITM attacks, ensuring that the data remains unreadable to attackers.
3. *Device Authentication:* Strong authentication methods between IoT devices and the blockchain network prevent unauthorized devices from communicating with the network.
4. *Secure Boot and Firmware Verification:* Ensuring IoT devices use secure boot and firmware verification protects devices from being compromised.
5. *Regular Software Updates:* Regularly updating software on IoT devices and the blockchain network protects against known vulnerabilities that attackers might exploit.

In preventing attacks, the identification of IoT devices is crucial. The identification process involves uniquely recognizing devices in the network using serial numbers and MAC addresses. Authentication includes using certificates, digital signatures, or other cryptographic methods to ensure the device's authenticity. Verifying device characteristics involves checking relevant data, such as sensor type, software version, security settings, and compliance with network security policies.

When a device with the necessary certificate accesses the blockchain network, there are several possibilities for data verification:

- *Initial Verification:* Involves thorough authenticity checks when the device first connects to the network.
- *Continuous and Periodic Checks:* Include certificate validation, security setting checks, and activity monitoring.
- *Transaction Verification:* Involves cryptographic methods for transaction verification, including digital signing and data hashing.
- *Smart Contracts:* Enable automated data verification processes during each transmission, including data authenticity checks and security policy implementation.

Proper security measures help reduce risks and ensure the safety of IoT devices and the blockchain network.

5. Integration of AI, Blockchain, and IoT for Enhancing Digital Security

The integration of Artificial Intelligence (AI), blockchain, and the Internet of Things (IoT) can significantly contribute to improving digital security, especially in the context of protecting financial systems and processes. Here are some key functions that these three areas can undertake when working together:

Artificial Intelligence (AI):

- *Pattern Recognition:* AI can analyze large amounts of data in real time to recognize suspicious behavior patterns indicative of fraud or attacks.
- *Automated Response:* AI can automatically respond to identified threats, enabling faster and more efficient incident responses.
- *Predictive Analytics:* Using historical data, AI models can predict potential threats and provide early risk warnings.

Blockchain:

- *Transparency and Data Integrity:* Blockchain provides immutable transaction records that are transparent and verified, reducing the likelihood of fraud.
- *Decentralized Security:* Instead of storing data in centralized locations vulnerable to attacks, blockchain distributes information across the network, increasing resilience to hacking.
- *Smart Contracts:* These self-executing contracts can automatically carry out transactions when conditions are met, reducing the possibility of human error and fraud.

Internet of Things (IoT):

- Device Connectivity: IoT enables the connection of various devices, ensuring that data from the physical world is integrated into digital processes. This can improve transaction efficiency and security.
- Threat Monitoring and Detection: Smart sensors can monitor activities and the current state of devices or systems, enabling quick detection and response to security threats.
- Data Collection: IoT devices generate large amounts of data that can be used for analysis and threat detection.

By combining AI, blockchain, and IoT technologies, organizations can create a robust framework for protecting their financial systems and processes. These technologies complement each other, enhancing predictive and reactive security measures, and reducing the risk of fraud and hacking. Additionally, such a system can increase trust among users and clients, thereby strengthening the overall digital security infrastructure.

6. Examples of AI, IoT, and Blockchain Integration

Most studies have focused on IoT and AI or IoT and blockchain integration [27]. The development of AI allows the integration of all three technologies, ensuring the security of the IoT network. Blockchain is immutable and distributed, making it resistant to hacking. AI and blockchain complement each other and reduce risks. An example of solutions that enhance digital trust by integrating AI, blockchain, and quantum-resistant security are the WISeKey solutions [28]:

- *WISeID:* A platform for digital identity and security (certification, e-signatures, and email protection).
- *SEALSQ:* A platform for secure digital identities and services.
- *WISeCoin:* A platform for tokenization and authentication.
- *SEALCOIN:* A platform for transactions between IoT devices.

Although according to ZACKS' ratings, WISeKey currently does not appear to be the most favorable investment option, the principles and technologies they are developing will still be relevant in the broader context of digital security and advanced technologies.

Products from other well-known manufacturers that integrate blockchain, AI, and IoT are:

1. *IBM:* IBM Watson, IBM Blockchain, IBM IoT.
2. *Microsoft:* Azure Blockchain Service, Azure AI, Azure IoT Hub.
3. *Intel:* Intel SGX, Intel IoT.
4. *Amazon Web Services (AWS):* Amazon Managed Blockchain, Amazon SageMaker, Amazon IoT Core.
5. *Huawei:* IoT devices and platforms.
6. Cisco Systems: Cisco Kinetic for IoT, Cisco Blockchain.

All these innovative solutions contribute to the field of digital security and efficiency.

7. Conclusions

The development of computer applications in finance brings benefits but poses security risks, necessitating continuous enhancement of protection measures. Improving digital security in the financial sector is possible using AI, IoT, and blockchain technology, and is most effective through their integration.

Artificial intelligence enables the recognition of suspicious behavior patterns through real-time analysis of large amounts of data, enhancing fraud detection. The AI's ability to automate threat responses allows faster and more efficient incident management. AI's predictive analytics can foresee potential threats based on historical data, enhancing proactive security measures.

The Internet of Things enables real-time data collection, helping financial institutions respond swiftly to changes and make data-driven decisions. IoT technology improves the security of financial transactions by monitoring network activities and identifying suspicious occurrences. Smart sensors track activities and the current state of devices, enabling quick detection and response to security threats.

Blockchain technology provides data integrity and transparency through decentralized ledgers, reducing the likelihood of fraud. The distributed nature of

DOI: https://doi.org/10.53486/ser2025.29
**International Scientific and Practical Conference,
4th Edition, March 27-28, 2025, Chișinău, Moldova**

blockchain enhances resilience to hacking attacks. Smart contracts enable transaction automation, minimizing the risk of human error and fraud.

Integration of AI, blockchain, and IoT technologies allows financial institutions to create a robust framework for protecting their systems and processes. These technologies complement each other, enhancing predictive and reactive security measures, and lowering the risk of fraud and hacking. Their integration increases trust among users and clients, strengthening the overall digital security infrastructure.

Based on the research and analysis, there is sufficient evidence to reject the null hypothesis. The findings support the alternative hypothesis, which states that integration of AI, IoT, and blockchain technology significantly improves digital security in the financial sector by enhancing fraud detection, automating threat responses, and ensuring data integrity.

Key Protection Recommendations

Each of these technologies offers many benefits to users, but none is perfect or immune to security weaknesses. The reasons are numerous, ranging from the rapid pace at which technologies develop, and the inability to comprehensively address every problem, to fundamental errors in the underlying solution concepts. It is also important to consider that specific software is developed by a small group of people, while software errors are explored by an army of attackers. However, there are effective protective solutions, such as:

- Using strong encryption methods for communication between IoT devices and the blockchain network.
- Implementing strong authentication methods between IoT devices and the blockchain network.
- Regularly updating software on IoT devices and the blockchain network to protect against known vulnerabilities.
- Applying security policies and verifying transactions using cryptographic methods.
- Automating data verification with smart contracts.

Implementing these solutions significantly reduces risks and complicates attackers' efforts.

8. References

[1] ČEKEREVAC, Z., BOGAVAC, M. *Impact of the pandemic on blockchain and the IoT application in supply chains from the SME aspect*. Mechanics Transport Communications, 2022, 20 (3/3), 11–17.

[2] CEKEREVAC, Z., CEKEREVAC, P. *Blockchain Technology and Application – SMEs Aspect*. MEST Journal, 2023, 11(2), 28–39. DOI: 10.12709/mest.11.11.02.04.

[3] MUTUM, P. S., BAGGA, N., KALRA, S., SINGH, S. *Advances and Perspectives in Quantum Cryptography: A Comprehensive Review*. International Journal of Scientific Development and Research (IJSDR), 2023, 677–683.

[4] HARTL, K., BRACK, F. *What is Zero Trust Architecture (ZTA)?* 2024. [Viewed 14 Jan. 2025]. Available from: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

[5] PC Press. *Tehnološki partner koji oblikuje budućnost sektora bankarstva*. [Viewed 14 Jan. 2025]. Available from: https://pcpress.rs/tehnoloski-partner-koji-oblikuje-buducnost-sektora-bankarstva/.

[6] HARRIS, C. *The Top 8 Continuous Security Monitoring Tools*. 2024, 07 May. [Viewed 14 Jan. 2025]. Available from: Expert Insights: https://expertinsights.com/insights/the-top-continuous-security-monitoring-tools/.

[7] MALETIC, J., CEKEREVAC, Z. *IIoT Security in Supply Chain*. Proceedings of the V International Scientific and Practical Conference "Scientific and Technical Aspects of Innovative Development of the Transport Complex". Doneck, 2019, 44–48.

[8] STANHAM, L. *Behavioral Analytics*. CrowdStrike. 2025, 16 Jan. [Viewed 15 Jan. 2025]. Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/behavioral-analytics/.

[9] MICROSOFT. *What is secure access service edge (SASE)?* Microsoft. [24 Feb. 2021]. [Viewed 15 Jan. 2025]. Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-sase.

[10] SWEENEY, P., GITTIEN, S. *What is identity and access management? Guide to IAM*. TechTarget. 2024. [Viewed 15 Jan. 2025]. Available from: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.

[11] WHITE, M. *AI arms race: How AI will be used by cyber-attackers (and defenders)*. Specops. [Viewed 15 Feb. 2025]. Available from: https://specopssoft.com/blog/ai-in-cybersecurity-arms-race-attackers-defenders/.

[12] MALATJI, M., TOLAH, A. *Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*. AI Ethics, 2024.

[13] ANTIĆ, M. *Digitalizacija donosi napredak, ali i nove izazove*. Banke & Biznis. 2024. [Viewed 16 Jan. 2025]. Available from: https://banke-biznis.com/mirko-antic-digitalizacija-donosi-napredak-ali-i-nove-izazove/.

[14] TECHBLOG. *Vodič za IoT u bankarstvu i Fintech-u*. TechBlog.co.rs. [11 Oct. 2022]. [Viewed 15 Jan. 2025]. Available from: https://techblog.co.rs/vodic-za-iot-u-bankarstvu-i-fintech-u/.

[15] NILAY, D. *How IoT Transforms Finance: Applications & Benefits*. 2024. Intuz. [Viewed 15 Jan. 2025]. Available from: https://www.intuz.com/blog/iot-impact-financial-services-industry.

[16] NASY, J. *IoT in Banking: Examples of IoT technology used in financial services*. Limestone Digital. [21 Apr. 2023]. [Viewed 15 Jan. 2025]. Available from: https://limestonedigital.com/iot-in-banking-examples-of-iot-technology-used-in-financial-services/.

[17] Admin. *IoT in Banking and Finance: Benefits, Use Cases and Real-World Examples*. Rishabh Software. [03 Jan. 2024]. [Viewed 17 Jan. 2025]. Available from: https://www.rishabhsoft.com/blog/iot-in-banking-and-finance.

[18] ČEKEREVAC, Z., et al. *SDD ITG 'smart shelf' RFID rešenje za inventarisanje robe na udaljenim policama [Eng. SDD ITG smart shelf RFID solution for the stocktaking of goods on remote shelves]*. IMK-14 - Istraživanje i razvoj, 2010, pp. 47–52.

[19] DELANEY, J. R., COLON, A. *The Best Smart Home Security Systems for 2025*. PC Mag. [Online 28 Jan. 2025]. [Viewed 15 Feb. 2025]. Available from: https://www.pcmag.com/picks/the-best-smart-home-security-systems.

[20] CEKEREVAC, Z., et al. *Hacking, protection and consequences of hacking*. Komunikacie Communications, 2018, 20(2), 83–87.

[21] INS_ADMIN. *IoT Security: 15 Types of Attacks with Real-World Examples*. Inova Sense. [Online 23 Oct. 2023]. [Viewed 15 Feb. 2025]. Available from:

https://www.inovasense.com/15-types-of-attacks-with-real-world-examples/?form=MG0AV3.

[22] MicroAI. *10 Types of Cyber Security Attacks in IoT*. Micro.ai. [Online 20 Aug. 2024]. [Viewed 05 Feb. 2025]. Available from: https://micro.ai/blog/10-types-of-cyber-security-attacks-in-the-iot.

[23] KONVERGE. *10 Types of Attacks on IoT*. Konverge Technologies. [Online 10 Aug. 2023]. [Viewed 05 Feb. 2025]. Available from: https://www.konverge.co.in/types-of-cyber-security-attacks-on-iot/.

[24] CEKEREVAC, Z., et al. *Techno-economic aspect of the Man-in-the-middle attacks*. Communications, 2017, 2, 166–172.

[25] CEKEREVAC, Z., PRIGODA, L., MALETIC, J. *Blockchain Technology and Industrial Internet of Things in the Supply Chains*. MEST Journal, 2018, 6(2), 39–47.

[26] CEKEREVAC, Z., CEKEREVAC, P. *Blockchain and the application of blockchain technology*. MEST Journal, 2022, 10(2), 14–25.

[27] ALHARBI, S., ATTIAH, A., ALGHAZZAWI, D. *Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends*. Sustainability, 2022, 14(23), p. 16002.

[28] CHOUCAIR, C. *WISeKey Unifies AI, Blockchain, and Quantum-Resistant Security to Strengthen Digital Trust*. Quantum Computing Business. [Viewed 18 Feb. 2025]. Available from: https://thequantuminsider.com/2025/02/18/wisekey-unifies-ai-blockchain-and-quantum-resistant-security-to-strengthen-digital-trust/.

[29] PALOALTO. *What Is Adversarial AI in Machine Learning?* Paloalto. [Online 12 Jun. 2024]. [Viewed 08 Feb. 2025]. Available from: https://www.paloaltonetworks.com/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning.