LEADING TECHNOLOGICAL INNOVATIONS IN DIGITAL SECURITY

CZU:
DOI:

Zoran Čekerevac
Independent Researcher, Belgrade, Serbia
zoran@cekerevac.eu
ORCID: 0000-0003-2972-2472

Lyudmila Prigoda
Maykop State Technological University, Maykop, Russian Federation
lv_prigoda@mail.ru
ORCID: 0000-0002-4762-3892

Petar Čekerevac
Independent Researcher, Belgrade, Serbia
petar.cekerevac@gmail.com
ORCID: 0000-0001-6100-5938

Abstract: Digital security holds critical importance in the era of global digitalization, which increasingly shapes daily life and business practices. Cyber threats such as ransomware, hacking, and data breaches demand continuous improvement of protective strategies to safeguard the integrity, confidentiality, and availability of information. Implementing advanced technologies has become essential for risk mitigation and enhanced system resilience. Innovations such as zero-trust architecture ensure access control and the elimination of implicit trust, while multi-factor authentication (MFA) significantly enhances system security. Artificial intelligence (AI) and machine learning (ML) enable real-time threat detection and response. At the same time, advanced cryptography, including post-quantum algorithms and homomorphic encryption, provides future-proof resilience against emerging threats. Technologies like blockchain and cloud security reduce administrative costs and enhance transparency, while specific protective measures for IoT devices and mobile platforms address their inherent vulnerabilities. Automation and *Security Orchestration, Automation*, and *R*esponse *(*SOAR*)* platforms optimize the efficiency of security teams, enabling faster incident responses. Efficient digital security requires a combination of cutting-edge technologies, user education, and continuous adaptation to the evolving threat landscape. A focus on the contextual needs of users ensures the successful implementation of protective measures. This paper the authors prepared using research methods typical of review articles, including the systematic processes of searching, selecting, analyzing, and synthesizing existing literature. The findings highlight that integrating AI, IoT, and blockchain technologies significantly fortifies digital security within the finance sector. Key benefits include enhanced fraud detection, automated threat response mechanisms, and improved data integrity. Recommended measures for bolstering security encompass advanced encryption protocols, robust authentication techniques, regular software updates, cryptographic validation of transactions, and the automation of smart contracts. Collectively, these technological advancements minimize vulnerabilities, deter malicious actors, and foster greater trust among users.

Keywords: Zero Trust Authentication, Blockchain, IoT, Post-Quantum Cryptography, Homomorphic Encryption, Ransomware.

JEL Classification: C88, D83, K24, L86, M15, O33

INTRODUCTION

Global digitalization has permeated every aspect of modern life, positioning digital security as critically important. With the increasing prevalence of cyber threats such as cyberattacks, hacking,

and ransomware, protecting data has become essential for individuals, organizations, and governments. As digital services grow and remote work becomes the norm, new vulnerabilities have emerged, offering cybercriminals opportunities to exploit them and underscoring the critical role of security risk management.

Furthermore, digital security is essential for ensuring compliance with data protection laws, such as the GDPR (2024). Companies now bear significant responsibility for safeguarding their users' data, as trust and reputation are often directly tied to their ability to prevent security incidents.

In an era where the boundaries between the physical and digital realms are increasingly blurred, security impacts everyday life—from online transactions and communications to critical infrastructure, such as energy, healthcare, and finance. Digital security is no longer merely a technical challenge; it is vital for maintaining the stability and safety of society.

1. Methodology

This study employs research methods typical of review articles, including systematic literature searches, selection, analysis, and synthesis. Sources identified were from academic sources like Google Scholar, IEEE Xplore, SpringerLink, and MDPI, alongside reputable websites focusing on information system security. Keywords such as Zero Trust Authentication, Blockchain, IoT, and Post-Quantum Cryptography guided the search.

The selection focused on relevance, quality, and recent publications, complemented by the inclusion of the authors' prior works on related topics. The authors thoroughly evaluated the papers, assessing their validity, reliability, and significance. Through thematic analysis, they uncovered key patterns, which led to the development of a conceptual framework that integrates existing knowledge while highlighting gaps. Bullet points ensured a concise and clear presentation of findings.

This methodology provides insights into digital security advancements while proposing directions for future research.

2. Research Question and Hypotheses

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

- *Research Question:* How does integrating advanced technologies such as AI, IoT, blockchain, post-quantum cryptography, and SOAR platforms influence digital security in the financial sector?
- *Null Hypothesis (H_0):* The advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) integration does not significantly enhance digital security in the financial sector.
- *Alternative Hypothesis (H_1):* The advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) integration significantly enhances digital security in the financial sector by improving fraud detection, automating threat responses, and ensuring data integrity.

KEY TECHNOLOGICAL INNOVATIONS

Organizations must ensure the security of their networks but also the confidentiality and integrity of their data, especially when dealing with sensitive information. Given attackers' ability to execute diverse and sophisticated attacks, the defense of digital systems requires advanced security measures. These measures must continually evolve as attackers also improve their methods daily. Security innovations are numerous, but they can be grouped and prioritized as follows (Authors, based on (Čekerevac & Radonjić, 2013; Cekerevac, et al., 2025; Brooks, 2010; Wong, et al., 2023; Jore, 2019)):

- Zero Trust architecture - fundamental security approach.
- Multi-factor authentication (MFA) - wide application.
- Artificial intelligence and machine learning - prevention.
- Advanced cryptography - resilience against future threats.
- Blockchain technology - data security.
- Cloud security - growth of cloud-based data).
- Security Information and Event Management (SIEM) - real-time monitoring.
- Mobile Device Management (MDM) platforms - mobile device protection.
- Security orchestration and automation - operational efficiency.

3. Zero Trust Authentication

Using the principle of "never trust by default, always verify", Zero Trust architecture represents a fundamental approach to digital security (Jena, 2023). The core idea behind this model is that access to resources is never automatically granted—even within an organization's network—requiring continuous verification of the identity and authority of every user and device.

The main components of the Zero Trust model include (Authors, based on (Dhiman, et al., 2024; Gambo & Almulhem, 2025; Hartl & Brack, 2024; Cekerevac, et al., 2025)):

- Micro-segmentation: Dividing the network into smaller zones to restrict potential attacker movements.
- Multi-factor authentication (MFA) - multi-layered user identity verification using additional factors such as mobile codes, biometrics, or token devices.
- Continuous monitoring, that is, the user and device activities constantly tracking to detect anomalies and unauthorized access attempts.
- Least privilege principle: Granting users only the minimum level of access required to complete their tasks, thereby reducing potential damage in case of compromise.
- The Zero Trust model is applied across various industries, ranging from healthcare institutions that protect sensitive patient data to airports, where ensuring infrastructure and operational security is critical**.**

4. Multi-factor Authentication

Multi-factor authentication (MFA) is a security process that requires users to verify their identity using two or more authentication factors, significantly enhancing protection levels. That means that, in addition to username and password, users must provide additional verification to access an account or service.

Authentication factors can include (Authors, based on (Abhishek, et al., 2013; Ometov, et al., 2018)):

1. Something the user knows: Information such as passwords, PINs, or answers to security questions.
2. Something the user has: Physical devices or resources the user possesses, such as:
   - A mobile phone (used to receive codes via SMS, authentication apps, or email).
   - A token device (hardware that generates one-time codes).
   - Smart cards.
3. Something the user is: This refers to biometric characteristics, such as:
   - Fingerprints.
   - Iris or facial scans.
   - Voice recognition.

4. Somewhere the user is / Someone the user knows. When attempting to log in:
    - The user enters their username and password.
    - The system requires an additional factor, such as a one-time code sent via SMS or a fingerprint scan.
    - Upon entering the additional factor, the user gains access.

For example, even if an attacker gains knowledge of a user's password, they cannot access the account because they lack the second factor, such as the user's phone or biometric data.

MFA is vital because it ensures:

- Enhanced security: Prevents unauthorized access, even if the password is compromised.
- Protection of sensitive data: Essential for banking and business systems, where confidential documentation is stored.
- Phishing resistance: Even if an attacker deceives a user into revealing their password, the second factor, typically, remains inaccessible.

5. Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are utilized for identifying patterns and anomalies in data, aiding in threat prevention and detection. AI plays a pivotal role in enhancing digital security, particularly in banks and government institutions, but it simultaneously serves as a tool for malicious actors.

On the positive side, AI in security offers several advantages (White, 2025; Malatji & Tolah, 2024). Among these is the ability to rapidly analyze large volumes of data in real time and identify suspicious activities, such as unauthorized access or unusual usage patterns. AI can also detect anomalies in network traffic that may indicate hacking attempts. By employing ML, AI can identify and block malware before it causes damage (Antić, 2024). Precise identity management and access control strengthen security, especially concerning sensitive information. Additionally, AI automates security checks and incident responses, reducing reaction time and increasing the efficiency of security teams.

However, from a user perspective, AI introduces certain risks. Malicious actors can leverage AI to develop sophisticated attack methods, such as phishing campaigns, adaptive malware, and deepfake technologies. Data analysis powered by AI can pose risks to privacy and security, especially when sufficient protective measures are lacking. Beyond technical challenges, ethical considerations arise, such as transparency and accountability in AI-driven decision-making.

Analyzing the potential applications of AI must always consider worst-case scenarios. Offensive AI attacks reveal their complex and dynamic nature, necessitating adaptive defensive mechanisms that AI can support. Every AI-driven attack has multidimensional implications, strategies, motivations, and societal consequences, significantly complicating protection and underscoring the need for even more advanced defensive methods.

Defensive AI employs AI techniques to safeguard computer systems and networks against attacks (e.g., anti-malware systems, intrusion detection systems—IDS). Offensive AI utilizes AI techniques to attack computer systems (e.g., developing new cyber-attacks, and automating the exploitation of existing vulnerabilities). Adversarial AI is maliciously used to exploit AI/ML systems and data, including poisoning training data and manipulating input data (Malatji & Tolah, 2024).

6. Advanced Cryptography

Advanced cryptography encompasses sophisticated techniques and algorithms to protect data and communications in modern digital systems. These methods address increasingly complex threats

and ensure security in various scenarios, including financial transactions, government secrets, and personal data. Advanced cryptographic techniques, such as quantum cryptography, enhance data security, making it more challenging for unauthorized parties to gain access.

One key aspect of advanced cryptography is the application of asymmetric algorithms, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which use a pair of keys—a public key and a private key—for encryption and decryption. These algorithms rely on mathematical problems, such as the factorization of large numbers or discrete logarithms, which are extremely difficult to solve without the appropriate keys. (Ahmed & Ahmed, 2022)

Post-quantum cryptography is becoming increasingly important with the development of algorithms designed to resist quantum computer attacks. These algorithms, including lattice-based and code-based methods, ensure the long-term security of data, even in the era of quantum computing.

Hash functions are another critical component of advanced cryptography. They are used to verify data integrity and create digital signatures. Hash functions, such as SHA-256, generate unique data summaries crucial for authentication and detecting unauthorized changes (Mironov, 2005).

Advanced cryptography encompasses techniques such as homomorphic encryption, enabling the processing of encrypted data without decryption, and zero-knowledge proofs, allowing claims to be verified without revealing any additional information.

These methods find application in areas such as blockchain technology, IoT device security, and cloud security.

7. Blockchain Technology

Blockchain technology enables decentralized and transparent data protection, ensuring its integrity and authenticity. It is ideal for securely storing and verifying transactions, reducing the risk of fraud and data manipulation (Cekerevac, et al., 2018).

In finance, blockchain plays a significant role by enabling transactions without time constraints, independent of banks and governments. Advances in hardware and communications accelerate transactions while increasing market capitalization stabilizes cryptocurrency values. Additionally, blockchain reduces transaction costs by eliminating intermediaries and reducing administrative requirements (Cekerevac & Cekerevac, 2022).

Blockchain technology is resistant to many attacks, including MITM attacks, but connected IoT devices may be compromised if they are not adequately secured (Cekerevac, et al., 2017). That can endanger blockchain, for example, through compromised data, manipulation of smart contracts, DDoS attacks, device identity theft, or ransomware attacks. Mitigating these risks requires the implementation of strong security measures for IoT devices and networks, along with ensuring the integrity of blockchain systems.

Preventing attacks requires secure communication between IoT devices and the blockchain network, encryption, authentication, secure system boot processes, and regular software updates. IoT device identification involves unique recognition through serial numbers and MAC addresses, while authentication utilizes certificates, digital signatures, or cryptographic methods to verify authenticity. Data verification includes checking sensor readings, software versions, and security configurations.

When a device with the appropriate certificate accesses the blockchain network, verification includes initial checks, continuous monitoring, cryptographic methods for transaction verification, and automated smart contract processes. Strong security measures help reduce risks and protect IoT devices and blockchain networks.

8. Cloud Security

An increasing volume of data is migrating to the cloud. Innovations in cloud security include improved access management, data encryption, and activity monitoring within the cloud. Key cloud security innovations encompass the Zero Trust approach, AI and machine learning, data encryption at rest and in transit, specific measures for container protection, security automation, post-quantum cryptography, and Secure Access Service Edge (SASE). SASE integrates network functions and security services into a unified platform, enabling safer cloud access from any location (Chen, et al., 2023).

A fundamental element of cloud security is multi-factor authentication (MFA), which facilitates multi-layered verification of user identities.

9. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) platforms are vital for real-time monitoring, analysis, and response to cyber threats, empowering organizations to act swiftly and decisively. Advanced technologies, such as artificial intelligence (AI) and machine learning (ML), enable the analysis of large data volumes, anomaly detection, and prediction of potential attacks. These capabilities contribute to automated responses and a reduction in reaction times. (González-Granadillo, et al., 2021)

The Zero Trust model increasingly contributes to ensuring controlled access to resources, while post-quantum cryptography and advanced encryption algorithms provide resilience against future quantum threats. These innovations make SIEM platforms more scalable, robust, and efficient in addressing modern cyber challenges.

10. Mobile Device Management (MDM) Platforms

Mobile Device Management (MDM) platforms allow organizations to manage and secure mobile devices that access corporate data. MDM requires cutting-edge technological advancements to fully protect data and devices in an increasingly complex digital environment. Key innovations include (Authors, based on (Glowinski, et al., 2020; Barthwal, 2016; Howell, et al., 2023)):

- Biometric authentication: Technologies such as facial recognition, fingerprint scanning, and voice analysis provide reliable user identity verification, reducing the risk of unauthorized access.
- Zero Trust model: Applied to mobile devices through continuous verification of user identity and authority, ensuring security even in environments with multiple access points.
- AI and machine learning: Artificial intelligence aids in the real-time detection of anomalies and threats, enabling rapid responses to potential attacks.
- Data encryption: Advanced encryption algorithms secure data during transmission and storage, mitigating the risk of information theft.
- Application management: MDM platforms employ technologies to control the installation and use of applications, preventing the spread of malware and unauthorized programs.
- Automated security checks: Automated processes allow for the rapid identification of mobile device vulnerabilities and the application of patches, reducing response times to incidents.

These innovations enhance MDM platforms' resilience against threats and improve their efficiency in protecting mobile devices and data.

11. Automation and Orchestration (SOAR)

Security Orchestration, Automation, and Response (SOAR) is an advanced framework designed to streamline and enhance cybersecurity operations. It integrates diverse security tools and

systems into a unified platform, centralizing management and coordination. By automating routine tasks, such as threat analysis and incident response, SOAR accelerates reaction times and reduces the burden on security teams, enabling them to focus on complex challenges. Additionally, SOAR leverages artificial intelligence and machine learning to analyze large datasets, detect anomalies, and predict potential cyber threats. These capabilities significantly improve the efficiency and precision of responses to incidents. Often operating in tandem with Security Information and Event Management (SIEM) platforms, SOAR uses collected and analyzed data to orchestrate and automate robust defense mechanisms. Its adoption is particularly beneficial for large organizations with intricate security environments, ensuring rapid and effective management of evolving threats. (Mir & Ramachandran, 2021; Bartwal, et al., 2022)

12. Priorities by User Groups

The innovations discussed play a vital role in strengthening digital security and protecting against increasingly sophisticated threats. An analysis of the security needs of organizations and individuals reveals varying priorities across user groups, depending on their size, industry, and exposure to threats:

1. Large Companies and Corporations:
   - Zero Trust architecture, in combination with SIEM systems, secures complex networks against internal and external threats, providing granular access control and real-time monitoring, which is critical for large organizations.
   - Automation and security orchestration are essential for companies aiming for rapid incident response while reducing manual effort.
2. SaaS Providers:
   - The Zero Trust model ensures secure cloud access for SaaS providers and protects data from unauthorized access.
   - AI and machine learning are crucial in real-time anomaly detection and threat identification.
   - Post-quantum cryptography ensures resilience against quantum computer attacks.
   - Secure Access Service Edge (SASE) technology integrates network functions and security services into a unified platform, enabling safer cloud access.
   - Security automation reduces incident response time.
   - Data encryption guarantees protection during transmission and storage.
   - Container security is crucial for protecting applications and data in dynamic environments.
3. Organizations Handling Sensitive Data:
   - Advanced cryptography, such as quantum cryptography or homomorphic encryption, is vital for banking, healthcare, and government.
   - Blockchain technology can secure transactions and ensure data integrity, especially in the financial sector.
4. Small Businesses and Individuals:
   - MFA offers a simple and effective solution for account protection.
   - Mobile Device Management (MDM) platforms help smaller firms protect employees' mobile phones and other devices.
5. Research and Advanced Centers:
   - Post-quantum cryptography and other cryptographic innovations are essential for institutes and organizations preparing for future threats, such as quantum computer

attacks. This field of cryptography focuses on developing algorithms that are more resistant to attacks from quantum computers.

POST-QUANTUM CRYPTOGRAPHY

With the development of quantum computers, the demand for new cryptographic techniques resistant to quantum attacks is becoming increasingly urgent. Due to their ability to solve specific mathematical problems much faster than classical computers, quantum computers are a potential threat to current cryptographic systems, particularly those based on public keys, such as RSA, ElGamal, and ECC.

Core Concepts of Post-Quantum Cryptography (Bernstein, et al., 2009; Dekkaki, et al., 2024):

a. *Resilience to Quantum Attacks*. Post-quantum algorithms aim to withstand threats from powerful quantum computers, ensuring security. For example, Shor's algorithm, utilized by quantum computers, can efficiently factorize large numbers, thereby compromising RSA encryption.

b. *Mathematical Approaches*. Post-quantum cryptography leverages mathematical problems that are challenging to solve, even for quantum computers, such as:

- Lattice-based cryptography: This approach uses mathematical structures known as lattices, arrays of points in multidimensional space. The foundation of security lies in the complexity of solving problems such as:
  - Shortest Vector Problem (SVP): Finding the shortest vector in a lattice.
  - Closest Vector Problem (CVP): Finding the closest vector to a target within a lattice. These problems pose significant challenges, remaining incredibly difficult to solve even for quantum computers. Lattice-based methods offer practical versatility, supporting encryption, digital signatures, and key exchange.
- Code-based cryptography: This method relies on error-correcting codes, primarily used for reliable data transmission. The security is based on the difficulty of decoding randomly generated codes. A well-known example, the McEliece algorithm, uses coding systems to create public and private keys. Advantages include resistance to quantum attacks and a high level of security, though key sizes can be significantly longer compared to other methods.
- Multivariate polynomial cryptography: This technique utilizes systems of multivariate polynomials as the foundation for encryption. The robustness of security relies on the intricate complexity of solving these systems, especially when numerous unknowns and parameters are involved. Multivariate polynomials are fast and energy-efficient, making them suitable for applications in resource-constrained environments, like IoT devices.

c. *Symmetric Encryption.* Symmetric algorithms, such as AES, remain relatively secure but require longer keys to maintain resilience against quantum attacks.

Each of these methods has its advantages and challenges, but they share a common goal: to provide resistance to attacks from quantum computers.

Post-quantum cryptography is essential because, once quantum computers become sufficiently advanced, they could undermine current cryptographic standards. That would have far-reaching implications for data security across financial, healthcare, and governmental sectors. Post-quantum cryptography is critical for ensuring future system resilience.

IoT SECURITY

IoT security is crucial due to the vulnerabilities and widespread adoption of IoT devices. These devices are often targets of attacks because of weaker security measures and the large number of

connected sensors. They can also be exposed to Man-in-the-Middle (MITM) attacks (Cekerevac, et al., 2017). Specific measures to enhance the security of Internet of Things (IoT) devices include:

1. *Strong authentication*: Multi-factor authentication (MFA) enhances security by ensuring controlled access to IoT devices, thereby reducing the risk of unauthorized entry. Default device passwords, which are commonly exploited in attacks, are intentionally avoided.
2. *Regular software updates*: Manufacturers frequently issue security patches for IoT devices. Regularly updated software reduces the risk of exploiting known vulnerabilities.
3. *Data encryption*: IoT devices and servers use encryption to secure transmitted data and prevent information interception.
4. *Network segmentation*: IoT devices should be separated from the core network, for example, by using a dedicated Wi-Fi network for IoT devices to reduce the risk of attack propagation (Baligodugula, et al., 2024).
5. *Anomaly monitoring and detection*: Tools monitor the activities of IoT devices to find any unusual behavior that might suggest a possible attack.
6. *Security protocols*: Protocols, like Transport Layer Security (TLS), are implemented for secure data transmission. VPNs provide additional protection for device communication. Moving away from VPNs exposes users to heightened security risks (Prigoda, et al., 2014).
7. *Physical security*: Physical protection of IoT devices is essential to prevent unauthorized access, particularly in industrial or public environments.
8. *Vulnerability testing*: IoT devices are regularly tested for security flaws using penetration testing tools or by engaging cybersecurity experts.

These measures reduce the risk of attacks and ensure the reliability of IoT devices.

HOMOMORPHIC ENCRYPTION

Homomorphic encryption is an advanced cryptographic technique that allows data to be processed and manipulated while still encrypted. This technology addresses a significant security challenge by enabling operations on data without decrypting it, thereby avoiding exposure to potential attackers.

The basic concept is as follows (Armknecht, et al., 2016; Gaid & Salloum, 2021):

- Despite encryption, data remains usable: Conventional methods require decryption, which can compromise security. Homomorphic encryption allows mathematical operations to be performed directly on encrypted data.
- The result remains encrypted: Once the operation is complete, the result remains encrypted, allowing the end user to decrypt it with a private key only when necessary.

Types of homomorphic encryption include (Sen, 2013; Buchanan, 2021; Pereira, 2016):

1. Partial homomorphic encryption:
   - Allows only specific types of operations (e.g., addition or multiplication) on encrypted data.
   - Example: RSA encryption supports multiplicative homomorphism.
2. Leveled homomorphic encryption:
   - Supports multiple types of operations but with a limited number of computational steps (calculation depth).
   - Used in scenarios where the number of operations needed is predetermined.
3. Full homomorphic encryption (FHE):
   - Allows any operation (addition, multiplication, etc.) on encrypted data without limitations.

- This technology is exceptionally effective but computationally intensive and still under development for broader applications.

Homomorphic encryption has immense potential in areas where data privacy is critical, such as:

- Healthcare: Doctors can analyze encrypted medical data without accessing patients' private information.
- Finance: Banks can process encrypted transactions without revealing sensitive data.
- Cloud services: Users can store encrypted data in the cloud and perform computations, ensuring the data remains fully protected.

However, there are limitations. Homomorphic encryption is resource-intensive in terms of processing power and time, but research and innovation in this field are advancing rapidly.

RANSOMWARE

Behavioral Analytics: Technologies that identify irregularities in user or system behavior to enable early threat detection. That is increasingly significant when combined with AI technologies. Ransomware protection consists of tools and strategies designed to detect and stop ransomware attacks.

Security programs recognize ransomware through a combination of techniques, including behavioral analysis, activity patterns, and real-time protection. The protection operates as follows (Guvçi & Şenol, 2023; Turaev, n.d.; Rehman, et al., 2024):

1. Behavioral Analysis:
   - Ransomware exhibits distinct behavior patterns, such as:
   - Encrypting large numbers of files within a short time frame.
   - Changing file extensions (e.g., .docx → .locked).
   - Creating "ransom notes."
   - Security software monitors these activities and utilizes heuristic methods to identify potential threats.
2. Threat Databases:
   - Antivirus programs use databases containing signatures of known ransomware types. When a file or process matches a known signature, the program blocks it immediately.
   - Regular updates to threat databases ensure recognition of new ransomware versions.
3. Machine Learning and AI:
   - Advanced security programs employ artificial intelligence (AI) to detect unknown threats. AI analyzes large datasets to learn how to identify suspicious behavior patterns.
   - For example, AI can detect new ransomware employing unconventional encryption methods.
4. Network Traffic Analysis:
   - Ransomware often communicates with command-and-control (C&C) servers to transmit encryption keys or receive commands.
   - Security tools analyze network traffic and block suspicious connections.
5. System Monitoring:
   - Programs monitor key directories and files for unexpected changes.
   - If unauthorized file modifications (such as encryption) are detected, the process can be stopped automatically.
6. Sandboxing (Isolation):

- When a suspicious file is executed, some security tools first run it in a "sandbox" environment (a virtual space) to analyze its behavior before allowing it access to the real system.

These protection functions also have a preventive aspect. Many security programs use proactive strategies, including:

- Blocking email attachments that may contain ransomware.
- Identifying fake URLs attempting to deceive users.

Ransomware protection is essential for preventing attacks that lock or encrypt user data until a ransom is paid. Key preventive measures include:

1. Regular backups. Periodically saving copies of important data on external devices or in the cloud to ensure data recovery without paying a ransom.
2. Software updates. Regular installation of security patches for operating systems and applications to eliminate known vulnerabilities.
3. Antivirus and anti-ransomware tools. Employing reliable security programs that can detect and block ransomware threats before any damage occurs.
4. User training. Comprehensive training tailored to participants' needs should cover:
   - Basics of advanced technologies: Training should include foundational principles of technologies like the Zero Trust model, AI and machine learning, post-quantum cryptography, data encryption, and Secure Access Service Edge (SASE).
   - Practical application: Focus on real-world examples and simulations to teach participants how to apply technologies, such as configuring Zero Trust architecture or managing SIEM platforms.
   - Threat recognition and response: Methods for identifying cyber threats, such as anomaly detection through AI algorithms, and procedures for reacting to various types of attacks.
   - Data protection: Educating participants on proper encryption techniques, key management, and the use of post-quantum algorithms to safeguard data during transmission and storage.
   - Cloud infrastructure security: Addressing challenges and solutions for securing hybrid and multi-cloud environments, including integrating network functions and protecting containers.
   - Ethics and regulations: Educating participants on the legal and ethical dimensions of digital security technologies, with a focus on privacy and transparency issues.
   - Incident management skills: Covering tools for automation (SOAR), coordinating security systems, and creating strategies for rapid incident response.

   This training supports the understanding and application of cutting-edge innovations in digital security, empowering participants to improve risk management and data protection efficiency. However, the depth of each topic depends on individual needs and their specific areas of work.
5. Network segmentation is crucial for enhancing digital security, as it divides IT infrastructure into smaller, controlled segments or zones. This approach improves system protection against cyber threats and minimizes the potential impact of attacks. Key aspects include:
   - Limiting attack spread: In segmented networks, potential attacks are localized within one zone, preventing attackers from accessing the entire infrastructure. For example, if one server is compromised, other parts of the network remain secure.

- Precise access control: Segmentation enables specific access rules for each zone, enhancing the protection of sensitive infrastructure against unauthorized users or systems.
- Simplified anomaly detection: Monitoring and analyzing traffic within segmented network areas facilitates the identification of suspicious activities and quick responses to incidents.
- Compliance with regulatory requirements: Network segmentation aids organizations in meeting data protection standards and regulations by isolating sensitive data and systems from the rest of the network.
- Performance optimization: Dividing the network into smaller zones improves traffic management and reduces load, enhancing overall efficiency.

Segmented networks are particularly beneficial in environments with complex IT structures, such as large organizations or financial institutions, where security and data control are priorities.

6. Access control. Access control is a fundamental pillar of digital security, ensuring that only authorized users and devices can access resources, applications, and data. Its primary role is to protect sensitive information from unauthorized access and potential misuse. Access control contributes to security through:
   - Restricting access: It facilitates system segmentation, determining who can access specific data or functions. For example, employees in different departments have distinct access rights, reducing the risk of accidental or intentional breaches. Applying the principle of least privilege limits access to only necessary resources for tasks, minimizing damage if ransomware compromises a user.
   - Identity verification: Multi-factor authentication (MFA) provides multi-layered user identity verification, significantly reducing the risk of unauthorized access and data breaches. MFA enables secure system entry and limits damage in case of user data compromise. This approach, combined with the adaptive features of the Zero Trust model, strengthens the overall security architecture, shielding organizations from ransomware and other threats. MFA is particularly critical in environments with sensitive data, including banking, healthcare, and cloud infrastructure.
   - Activity monitoring: Access control systems log and monitor login attempts and other activities, enabling rapid responses to suspicious actions or security incidents.
   - Protection against cyber threats: Prevents unauthorized access by attackers attempting to exploit stolen passwords, identities, or system vulnerabilities.
   - Compliance with legal regulations: Helps organizations align with privacy and data protection standards, such as GDPR or HIPAA.
   - Dynamic adaptation: Modern access control systems utilize Zero Trust models and adaptive approaches, which assess user behavior in real time and adjust access levels based on risk analysis.

   Access control is not merely a technical measure but also a strategic tool for managing security risks in organizations of all sizes.

Implementing these measures can significantly reduce ransomware attack risks and help protect data. These innovations enable organizations to secure their cloud data and infrastructure against increasingly sophisticated threats.

CONCLUSION

Digital security plays a crucial role in preserving the integrity, confidentiality, and availability of data in an era of growing digitalization. A combination of traditional methods and modern technological innovations has become essential for effectively protecting individuals, organizations, and governments from increasingly sophisticated cyber threats.

Zero Trust architecture is a fundamental principle that eliminates implicit trust and ensures continuous verification of every access to resources. This model, together with multi-factor authentication (MFA), enhances security in environments encompassing mobile devices, cloud infrastructure, and sensitive data. Post-quantum cryptography and homomorphic encryption are becoming key for resilience against future quantum computer threats, enabling secure data processing.

Blockchain technology and cloud security contribute significantly to decentralized protection and cost optimization, while IoT devices, due to their vulnerabilities, require specific measures such as network segmentation and regular software updates. Security Information and Event Management (SIEM) platforms, combined with security orchestration and automation (SOAR), enable faster threat response and reduce manual workload.

The analysis highlights differences in user priorities by category. For instance, MFA and MDM platforms play a vital role for small businesses and individuals, while advanced technologies such as Zero Trust architecture, SIEM systems, and post-quantum cryptography are indispensable for large corporations, SaaS providers, and research centers.

Nevertheless, advanced systems do not diminish the importance of fundamental security practices. User training, regular data backups, and software updates remain essential for attack prevention. Digital security requires an integrated approach that combines cutting-edge technologies with practical strategies, adapting continuously to the evolution of threats.

The conclusion emphasizes the need for education and ongoing improvement to prepare individuals and organizations for future challenges. A balance between innovation and fundamental security measures ensures protection that is not only effective but also sustainable in an ever-changing world.

Based on the research and analysis, there is sufficient evidence to reject the null hypothesis. The findings support the alternative hypothesis, which states that integrating advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) significantly enhances digital security in the financial sector by improving fraud detection, automating threat responses, and ensuring data integrity.

REFERENCES

Abhishek, K., Roshan, S., Kumar, P. & Ranjan, R., 2013. *A Comprehensive Study on Multifactor Authentication Schemes.* Berlin, Springer, pp. 561-568.

Ahmed, S. & Ahmed, T., 2022. Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review. *International Journal of Scientific and Research Publications,* 12(7), pp. 161-173.

Antić, M., 2024. *Digitalizacija donosi napredak, ali i nove izazove.* [Online] Available at: https://banke-biznis.com/mirko-antic-digitalizacija-donosi-napredak-ali-i-nove-izazove/

Armknecht, F. et al., 2016. *A Guide to Fully Homomorphic Encryption.* [Online] Available at: https://eprint.iacr.org/2015/1192.pdf [Accessed 02 04 2025].

Baligodugula, V. V., Ghimire, A. & Amsaad, F., 2024. An Overview of Secure Network Segmentation in Connected IIoT Environments. *Computing & AI Connect,* Issue 1, p. Article ID: 0004).

Barthwal, D., 2016. *Mobile Device Management (MDM) in Organizations.* [Online] Available at: https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations [Accessed 03 04 2025].

Bartwal, U., Mukhopadhyay, S., Negi, R. & Shukla, S., 2022. *Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots.* s.l., arXiv:2201.05326 [cs.CR], p. 8.

Bernstein, D. J., Buchmann, J. & Dahmen, E., 2009. *Post-Quantum Cryptography.* Berlin Heidelberg: Springer.

Brooks, D. J., 2010. What is security: Definition through knowledge categorization. *Security Journal,* Volume 23, pp. 225-239.

Buchanan, B., 2021. *On Global Encryption Day: A Practical Guide to Homomorphic Encryption.* [Online] Available at: https://asecuritysite.com/blog/2021-10-22_On-Global-Encryption-Day--A-Practical-Guide-to-Homomorphic-Encryption-be5670240900.html [Accessed 01 04 2025].

Cekerevac, Z. & Cekerevac, P., 2022. Blockchain and the application of blockchain technology. *MEST Journal,* 15 07, 10(2), pp. 14-25.

Cekerevac, Z., Cekerevac, P., Prigoda, L. & Naima, F. A., 2025. Security Risks from the Modern Man-In-The-Middle Attacks. *MEST Journal,* 15 01, 13(1), pp. 34-51.

Cekerevac, Z., Dvorak, Z., Prigoda, L. & Cekerevac, P., 2017. Internet of things and the Man-In-The-Middle attacks – Security and economic risks. *MEST Journal,* 5(2), pp. 15-25.

Cekerevac, Z., Prigoda, L. & Cekerevac, P., 2025. *Enhancing Digital Security in the Financial Sector With AI, IoT, and Blockchain.* Chisinau, Moldova, s.n.

Cekerevac, Z., Prigoda, L. & Maletic, J., 2018. Blockchain Technology and Industrial Internet of Things in the Supply Chains. *MEST Journal,* 15 July, 6(2), pp. 39-47.

Chen, R. et al., 2023. *Overview of the Development of Secure Access Service Edge.* Singapore, s.n.

Čekerevac, Z. & Radonjić, S., 2013. *Some SMEs data safety and security issues in the in-house and in the cloud computing.* Žilina, Slovakia, s.n.

Dekkaki, K. C., Tasic, I. & Cano, M.-D., 2024. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies,* 12(12), p. 242.

Dhiman, P. et al., 2024. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors,* 24(4), p. 1328.

Gaid, M. L. & Salloum, S. A., 2021. *Homomorphic Encryption.* Settat, Morocco, s.n., pp. 634-642.

Gambo, M. L. & Almulhem, A., 2025. *Zero Trust Architecture: A Systematic Literature Review.* [Online] Available at: https://arxiv.org/abs/2503.11659 [Accessed 03 04 2025].

GDPR, 2024. *General Data Protection Regulation (GDPR).* [Online] Available at: https://gdpr-info.eu/ [Accessed 03 04 2025].

Glowinski, K., Gossmann, C. & Strümpf, D., 2020. Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. *SN Appl. Sci.,* 2(42).

González-Granadillo, G., González-Zarzosa, S. & Diaz, R., 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors,* 21(14), p. 4759.

Guvçi, F. & Şenol, A., 2023. An Improved Protection Approach for Protecting from Ransomware Attacks. *Journal of Data Applications,* 02 08, 0(1), pp. 69-82.

Hartl, K. & Brack, F., 2024. *What is Zero Trust Architecture (ZTA)?.* [Online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Howell, G. et al., 2023. *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Gaithersburg, MD: NIST Special Publication SP 800-124r2.

Jena, K., 2023. Zero-Trust Security Models Overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 9(6), pp. 70-76.

Jore, S., 2019. The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *Eur J Secur Res,* Issue 4, p. 157–174.

Malatji, M. & Tolah, A., 2024. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI Ethics,* 15 02.

Mir, A. W. & Ramachandran, R. K., 2021. *Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems.* Singapore, Springer, pp. 157-169.

Mironov, I., 2005. *Hash functions: Theory, attacks, and applications,* Mountain View, CA: Microsoft Research, Technical Report.

Ometov, A. et al., 2018. Multi-Factor Authentication: A Survey. *Cryptography,* 2(1), p. 1.

Pereira, H. V. L., 2016. *Difference between leveled FHE and normal FHE scheme.* [Online] Available at: https://crypto.stackexchange.com/questions/15794/difference-between-leveled-fhe-and-normal-fhe-scheme [Accessed 01 04 2025].

Prigoda, L., Cekerevac, Z., Dvorak, Z. & Cekerevac, P., 2014. One Look at the Modern Information Security. *Sustainable Development of Mountain Territories,* 4(22), pp. 99-103.

Rehman, M., Akbar, R., Omar, M. & Gilal, A., 2024. *A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks.* Singapore, s.n.

Sen, J., 2013. *Homomorphic encryption-theory and application.* Rijeka, Croatia: IntechOpen.

Turaev, H., n.d.. *Literature Review on Ransomware and Approaches to Its Mitigation.* [Online] Available at: https://www.academia.edu/32167535/Literature_Review_on_Ransomware_and_Approaches_to_Its_Mitigation [Accessed 01 04 2025].

White, M., 2025. *AI arms race: How AI will be used by cyber-attackers (and defenders).* [Online] Available at: https://specopssoft.com/blog/ai-in-cybersecurity-arms-race-attackers-defenders/

Wong, R., Morris, K. & Masys, A. J., 2023. Safety and Security Science and Technology. In: *Safety and Security Science and Technology: Perspectives from Practice.* s.l.:Springer, Cham, pp. 127-139.