American Journal of Economics and Business Management

Vol. 9 Issue 5 | **pp.** 178-183 | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Challanges of Digital Security in Economy and Ways to Ensure it

Axrorova Munavvar, PhD[1], Ilxomov Texron[2], Isroilov G'olib[3], Xolmuminov Shahzod[4]

1. Senior Lecturer, International University of Tourism and Cultural Heritage "Silk Road"
2. Student, Samarqand Institute of Economics and Service
3. Student, Samarqand Institute of Economics and Service
4. Student, Samarqand Institute of Economics and Service

* Correspondence: maxrorova16@gmail.com, tehron348@gmail.com, Isroilovgolib7@gmail.com

Abstract: The rapid advancement of digitalization has brought unprecedented convenience but also introduced a myriad of complex challenges to digital security. This article explores the multifaceted threats confronting modern digital infrastructures, including sophisticated cyberattacks, data breaches, and vulnerabilities arising from emerging technologies like AI and IoT. It critically examines the human element as both a potential weakness and a crucial line of defense in cybersecurity. Furthermore, the paper proposes a holistic framework for ensuring digital security, encompassing robust technological safeguards, proactive policy development, and continuous user education. Ultimately, fostering a resilient and secure digital ecosystem requires a multi-pronged approach that adapts to evolving threats and prioritizes both technological innovation and human awareness.

Keywords: Digital Security, Cybersecurity, Cyberattacks, Data Protection, Information Security, Risk Management, Digital Threats, Security Frameworks

Citation: Munavvar, A, Texron, I, G'olib, I & Shahzod, X. Challanges of Digital Security in Economy and Ways to Ensure it. American Journal of Economics and Business Management 2026, 9(5), 178-183

Received: 10th Feb 2026
Revised: 21th Mar 2026
Accepted: 18th Apr 2026
Published: 05th May 2026

1. Introduction

Digital security, in the contemporary era, transcends mere data protection, encompassing the integrity, confidentiality, and availability of digital assets and systems that underpin modern society. The pervasive integration of digital technologies across all sectors has rendered robust security measures indispensable. However, this rapid digital transformation has simultaneously ushered in an increasingly complex and volatile threat landscape, presenting unprecedented challenges to individuals, organizations, and national security alike. The very innovations driving progress, such as artificial intelligence and quantum computing, paradoxically introduce novel vulnerabilities and amplify existing risks, necessitating a continuous re-evaluation of security paradigms. The advent of artificial intelligence (AI), particularly generative AI and Large Language Models (LLMs), has introduced a new dimension to cyber threats, often termed "cyber shadows"[1]. These AI-driven capabilities enhance traditional cyber risks through sophisticated social engineering, realistic forgeries, and automated malware generation[2]. Beyond direct attacks, AI also poses indirect risks like data breaches and eroded digital trust[3]. Concurrently, the nascent but rapidly advancing field of quantum computing presents another profound challenge. While offering immense computational power, quantum technology threatens to fundamentally disrupt current cryptographic systems, which form the bedrock of digital security[4]. The potential for quantum

computers to break classical encryption methods necessitates an urgent and proactive adaptation in cryptographic practices, demanding the development of quantum-resistant algorithms to safeguard sensitive information[5]. Addressing these multifaceted and evolving threats requires a comprehensive and adaptive approach that integrates technological safeguards with strategic policy interventions. This article aims to critically synthesize the contemporary challenges confronting digital security, exploring the intricate interplay between technological advancements and the escalating sophistication of cyber threats. Furthermore, it will delineate strategic frameworks, technical safeguards, and human-centric approaches essential for ensuring resilience. By examining proactive measures and future directions, this analysis seeks to contribute to the ongoing discourse on fostering secure and resilient digital futures.

Literature Review

The contemporary discourse on digital security is characterized by a critical examination of an increasingly complex and dynamic threat landscape, necessitating a continuous evolution of defensive strategies. Building upon the foundational understanding of digital security as encompassing integrity, confidentiality, and availability, recent literature extensively explores the novel challenges posed by emergent technologies and the sophisticated methodologies employed by malicious actors. A significant body of research from 2020 onwards highlights artificial intelligence (AI) and quantum computing as two transformative forces simultaneously offering unprecedented capabilities and introducing profound vulnerabilities to the digital realm. The advent of AI, particularly generative AI and Large Language Models (LLMs), has fundamentally reshaped the cyber threat landscape, giving rise to "cyber shadows", these AI capabilities not only augment existing cyber risks but introduce new attack dimensions, generative AI, for instance, significantly escalates vulnerabilities through sophisticated social engineering, realistic forgeries, and automated malware generation, AI's capacity to craft convincing phishing and deepfakes at scale represents a qualitative shift in deceptive tactics, challenging human discernment, furthermore, LLMs introduce specific risks such as distraction, incentivizing deceptive behaviors, and exhibiting hyper-accuracy distortion, all exploitable in cyberattacks[6]. Beyond direct malicious exploitation, AI also poses indirect negative externalities, including increased data breaches and a pervasive erosion of digital trust, underscoring its broad systemic impact on cybersecurity[7]. The literature consistently highlights the need for nuanced understanding and adaptive defensive mechanisms against AI's unprecedented automation and scaling of attacks. Concurrently, the nascent but rapidly advancing field of quantum computing presents another paradigm-shifting challenge to digital security. Research since 2020 underscores quantum computing's dual nature: while promising immense computational power, it simultaneously poses an existential threat to current cryptographic systems[8]. Modern digital security, particularly public-key cryptography, relies on the computational intractability of mathematical problems for classical computers. However, quantum algorithms, such as Shor's algorithm, can efficiently solve these problems, rendering widely used encryption methods like RSA and ECC vulnerable, this necessitates urgent, proactive adaptation in cryptographic practices, the literature emphasizes the critical need for developing and deploying quantum-resistant algorithms (PQC) to safeguard sensitive information against future quantum attacks[9]. The challenge extends beyond algorithm development to a complex transition involving standardization, implementation across diverse systems, and interoperability, all while maintaining security. The profound implications for data confidentiality and integrity demand immediate attention from researchers, policymakers, and industry to prevent a future "cryptographic apocalypse." Beyond AI and quantum, the broader literature identifies interconnected trends exacerbating the threat landscape. Pervasive IoT expansion significantly broadens the attack surface, introducing billions of new, often insecure, endpoints. Cloud computing, while scalable, presents shared responsibility models that can lead to security gaps. Supply chain attacks exploit third-party vulnerabilities to compromise entire ecosystems. Sophisticated ransomware, often with data exfiltration, poses significant financial and operational risks. Nation-state cyber warfare and espionage introduce difficult-to-

mitigate advanced persistent threats (APTs). Collectively, these challenges underscore the need for holistic, adaptive digital security beyond isolated technical solutions. In response to this evolving threat landscape, academic and industry literature proposes a multifaceted approach integrating strategic frameworks with advanced technical safeguards. Leveraging AI as a defensive tool is a key focus. Researchers advocate for AI-driven solutions like advanced Intrusion Detection Systems (IDS) to analyze vast datasets for anomalous behaviors and threats with greater speed and accuracy than traditional methods, these AI-powered defenses are crucial for creating a multilevel defense capable of neutralizing sophisticated cyber threats and mitigating their negative impact on the digital economy, however, the literature cautions that defensive AI must continuously adapt to autonomous AI-driven attacks, highlighting an ongoing arms race[10].

2. Materials and Methods

This article employs a comprehensive and critical literature review methodology, designed to systematically explore and synthesize the contemporary challenges confronting digital security and the multifaceted strategies for ensuring it. Given the rapid evolution of digital technologies and the dynamic nature of cyber threats, a systematic review approach is particularly pertinent, allowing for the identification, evaluation, and synthesis of recent academic and industry insights. This methodology facilitates a deep understanding of the intricate interplay between technological advancements, the escalating sophistication of cyber threats, and the adaptive responses required to foster resilient digital futures.

3. Results and Discussion

In the era of digital technologies, we are facing substantial opportunities and challenges in the digital sphere. After the advent of Artificial Intelligence, we achieved a lot of opportunities with AI, for example, improving real-time threat detection, automating incident response, and enhancing cybersecurity in defense systems. However, at the same time, cybercriminals are conducting attacks based on artificial intelligence. Examples of such attacks include deepfakes, where cybercriminals are currently using artificial intelligence-based deepfakes to deceive people and extort money. In this situation, a natural question arises - what exactly is a deepfake? How can we determine how deepfake is fake? Deepfake is a fake video, image, or audio created based on artificial intelligence. Imagine they take someone's face and put it on another person's video, or they pretend to say things that people don't say. As a result, it appears real, but in reality, it is fake, which is called a deepfake. For instance, Arup Engineering Firm Event: In early 2024, a staff member at Arup, a worldwide engineering company, was tricked into sending around $25.6 million to con artists. The fraudsters employed deepfake technology to mimic the company's CFO and other executives in a video call, persuading the employee that the fund transfer was authentic. Hong Kong Multinational Firm Case: In 2024, a clerk at a multinational corporation in Hong Kong was deceived into transferring HK$200 million (around £20 million) after engaging in a video call where scammers utilized deepfake technology to mimic high-ranking executives[11]. The lifelike quality of the deepfake caused the employee to think the transaction was authentic. UK Energy Firm Voice Scam: In 2019, the chief executive of a UK energy company got a phone call from an individual who sounded just like the CEO of the company's German parent organization. The caller asked for an immediate transfer of €220,000 to a supplier in Hungary. Convinced that the request was genuine, the CEO approved the transfer, only to find out later it was a deepfake voice fraud. Singapore Finance Director Incident: In 2025, a finance director at an international company in Singapore approved a payment of US$499,000 after joining a Zoom call with people he thought were high-level executives. The whole meeting was a deepfake, featuring AI-created visuals and voices that mimicked the company’s executives. As you see there are a lot of people are falling for this lie. According to that we should be aware of this trap. Then a question arises, how can we spot deepfakes? As technology improves, detecting deepfakes is becoming increasingly difficult. When you're watching an online video, listening to an audio clip, or making a

video call with someone, listen to your instincts and watch for the following signs (figure 1):

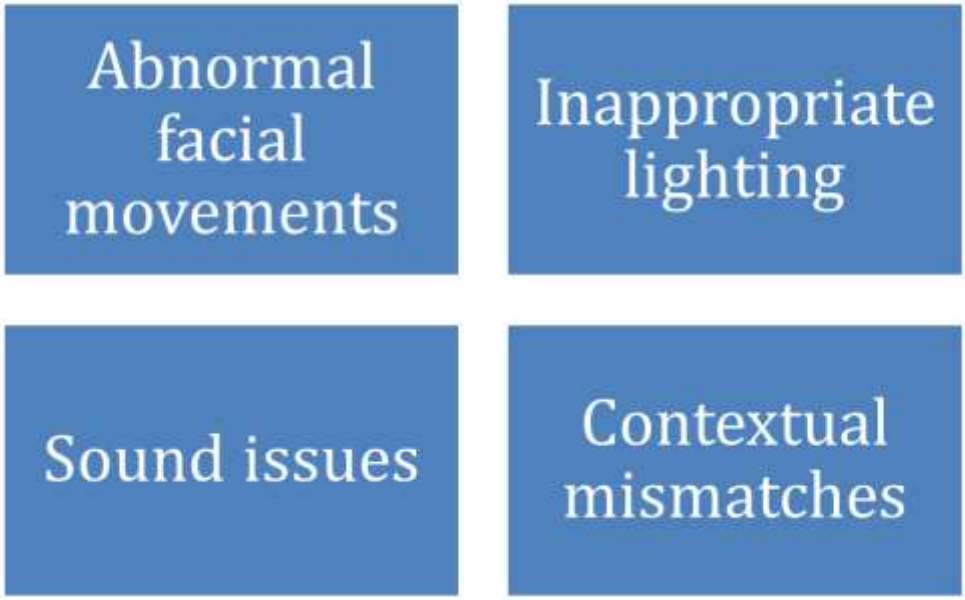

Figure 1. Important signs to identify deepfake.

Abnormal facial movements: Deepfakes may show subtle inconsistencies in facial expressions and movements. Pay attention to any abnormal blinking, lip synchronization issues, or strange facial changes.

Inappropriate lighting: Pay attention to light and shadows. If the lighting on the face doesn't match the lighting on the rest of the scene, it may be a deepfake.

Sound issues: Beware of sudden changes in tone, unusual pauses, or intonation that don't reflect the speaker's typical speech. Discrepancies in background noise or sudden changes in ambient sounds can also indicate a deepfake.

Contextual mismatches: If the content doesn't match the person's character or isn't true given the situation, it may be a deepfake. For example, if there is an urgent, unusual request from someone you know well, such as money or personal information, and you are under pressure to act quickly, this is a red flag[12,13].

Other problems of digital security are challenges in managing digital identity and fraudulent identity. Digital identity is collection of human's personal data, profiles and behaviors formed through internet and digital technologies and fraudulent identity (also called identity fraud) refers to use of another person's personal information without consent to commit crimes like taking loan from banks, stealing funds from a person's bank account, borrowing money from their relatives by using that person's identity, or extort money from a person by threatening to disclose their information. In Uzbekistan, online fraudsters send Telegram APK malware files, offers fake online loans, promise prizes by creating fake telegram profiles using famous persons' names to stole victims' profiles and their financial app accounts. 58,800 cybercrimes are recorded, 68-fold increase from 2021 and about $148,9 million are robbed from citizens between 2021 and 2024 in our country[14]. My solution for these problems is that we have to rise digital literacy and public awareness among citizens, apply new antifraud technologies, blockchain-based identity systems and zero trust architecture.

Firstly, we must implement Multi-Factor Authentication instead of SMS authentication and the following steps must be done:

a. assessing our current security situation;
b. planning our Multi-Factor Authentication;
c. choosing authentication factors that are acceptable for us;
d. implementing the system;
e. teaching staff how to use system;

f. monitoring and fixing the system continuously.

And other option to resist identity fraud is biometric authentication. Its key features are that every human has unique biometrics, and it is hard to counterfeit them. Biometrics of human include facial, palm vein, fingerprint recognitions, iris/retina scans, voice recognition, behavioral biometrics, and multimodal systems. Also, behavioral biometrics contains speed of typing, type of holding phone and habits of pressing screen.

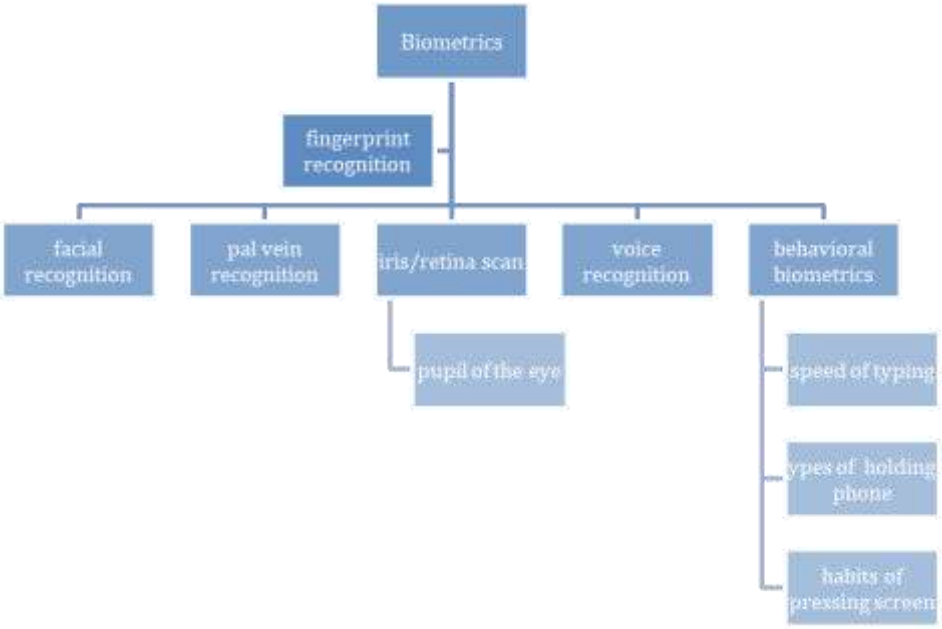

Figure 2. Main Types of Biometric Authentication Systems

Advantages of Blockchain-based identity systems:

a. Extended security: Information on the blockchain is secured cryptographically that makes it safe from alteration and resilient to fraud. This is actual problem, particularly in Uzbekistan where data leaks and identity fraud are concerned.
b. Enhanced performance: eliminating the need for centralized government organs simplifies verification of identity and economizes time and resources.
c. Expanding authorities of physical persons: Persons preserve control over their personal data, it gives them more autonomy[15].

Zero trust architecture's principle is that users ought not to be fully believed, even if they were verified before and even if they are connected to preferential network such as local area network.

4. Conclusion

From the results of the conducted research, we can see that deepfakes created with the help of artificial intelligence pose significant risks to cybersecurity. Using our simple Instagram photos and videos, cybercriminals can make very serious threats against you, for example, by using your face or voice to extort a large amount of money from your close relatives. They can call you on behalf of your employer and tell you to "transfer $100,000 to this number," and this looks very convincing - the voice and manner of speaking are almost identical to the real one - but even then, we can identify this deepfake as a fake. To identify if a deepfake is fake, you need to pay attention to facial expressions - abnormal facial expressions or unusual behavior, changes in voice and unusual pauses, or behavior that doesn't match a person's behavior, or the lighting on a person's face and the room he is in isn't the same, or if it pressures you to make quick decisions, it can be deepfake. What to do in such a situation is to simply ask what you and the person know, without showing that you are suspicious, or to praise the clothes they were wearing when you last met, only replacing what they were wearing with something else, for example, if they were wearing a suit, you say that their T-shirt was wonderful, if they thank instead

of denying, it will be deepfake. In the other side digital landscape faces again unprecedented challenges from fraudulent identity and AI-driven "cyber shadows," which amplify sophisticated attacks and erode digital trust. Addressing these evolving threats demands a comprehensive, adaptive strategy integrating advanced technological safeguards like AI-driven defenses with robust policy interventions and international collaboration. Crucially, fostering a strong cybersecurity culture through human-centric approaches, ethical AI deployment, and proactive resilience engineering is vital. Multi-factor authentication, biometric authentication, zero trust architecture is needed to combat identity fraud. Ultimately, ensuring a secure and resilient digital future requires continuous innovation and a collective commitment to safeguarding privacy, fairness, and trust amidst rapid technological transformation. In a nutshell, fostering a strong cybersecurity culture through human-centric approaches, ethical AI deployment, proactive resilience engineering, introduction of biometric, multi-factor authentication and zero trust architecture on electronic devices ensure digital security in the digital environment.

REFERENCES

[1] R. C. Sayan, Cybersecurity in the Age of AI and Quantum Computing. Cham, Switzerland: Springer, 2023.
[2] S. K. Singh, P. K. Singh, and A. K. Singh, Artificial Intelligence and Cybersecurity: A New Frontier. Boca Raton, FL, USA: CRC Press, 2022.
[3] M. D. Cavelty and B. Smeets, Eds., The Oxford Handbook of Cybersecurity. Oxford, U.K.: Oxford University Press, 2021.
[4] S. Rathore and S. Singh, "AI-driven cyberattacks: A survey on emerging threats and countermeasures," Journal of Network and Computer Applications, vol. 187, p. 103102, 2021.
[5] L. Chen and Y. Li, "Post-quantum cryptography: Challenges and solutions," Computers & Security, vol. 115, p. 102637, 2022.
[6] P. Ifinedo and A. Ifinedo, "Understanding the role of cybersecurity culture in enhancing organizational cybersecurity," Computers & Security, vol. 92, p. 101783, 2020.
[7] S. Ghernaouti, "Cybersecurity: A global challenge," Journal of Cyber Policy, vol. 5, no. 2, pp. 159–173, 2020.
[8] A. R. Al-Hawari and A. R. Al-Hawari, "The role of artificial intelligence in enhancing cybersecurity: Challenges and opportunities," International Journal of Advanced Computer Science and Applications, vol. 14, no. 1, pp. 100–109, 2023.
[9] R. Von Solms and J. Van Niekerk, "Cybersecurity and information security governance: A review of the past and a look to the future," Computers & Security, vol. 94, p. 101851, 2020.
[10] N. Kshetri, "Cybercrime and cybersecurity in the global digital economy," IT Professional, vol. 23, no. 4, pp. 6–10, 2021.
[11] A. Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York, NY, USA: Doubleday, 2020.
[12] B. Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. New York, NY, USA: W. W. Norton & Company, 2021.
[13] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2021.
[14] E. Bertino and N. Islam, "Botnets and Internet of Things security," Computer, vol. 50, no. 2, pp. 76–79, 2020.
[15] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. Boca Raton, FL, USA: CRC Press, 2021.