Journal of Artificial Intelligence and Technology, (Ahead of Print)
https://doi.org/10.37965/jait.2025.0881

ISTP
RESEARCH ARTICLE

Enhancing Security in Operational Technology: The Role of Multi-Factor Authentication Against Cyber Threats

Albandari Alsumayt,[1] Nahla El-Haggar,[2] Majid Alshammari,[3] Fatemah H. Alghamedy,[2] and Zeyad AlFawaer[4]

[1]Saudi Aramco Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[2]Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
[4]Department of Science Technology and Mathematics, College of Art and Sciences, Lincoln University, Jefferson City, MO, USA

(Received 27 July 2025; Revised 22 September 2025; Accepted 27 October 2025; Published online 15 November 2025)

Abstract: As cyber threats continue to increase in sophistication, the security of Operational Technology (OT) environments has become a paramount priority for organizations in various sectors. OT systems, including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, are vital in the functioning of critical infrastructure but often lack robust security due to legacy security weaknesses. This research discusses the implementation of Multi-Factor Authentication (MFA) as a baseline strategy for enhancing the security of such systems. We recognize the distinct cybersecurity issues of OT environments, especially the use of legacy hardware that does not have contemporary security mechanisms. By suggesting an extensive framework for implementing MFA, this research offers a multi-layered system that incorporates knowledge-based, possession-based, and biometric authentication techniques. We further stress the need for role-based access control, ongoing monitoring, and user training to enhance security mechanisms. Using case studies and real-world examples, we show how MFA can be used to counter unauthorized access and increase system resilience. We present actionable recommendations for organizations wishing to deploy MFA, including mitigation strategies that reduce identified vulnerabilities to acceptable levels for critical infrastructure as a foundation of their cybersecurity approach, with the ultimate goal of safeguarding critical infrastructure and sensitive information in a hyper-connected world. Our research not only adds to the body of knowledge but also acts as a guide to deploying stringent security controls in OT networks.

Keywords: authentication; cybersecurity; IT/OT convergence; MFA; Operational Technology (OT); SFA; 2FA

I. INTRODUCTION

Operational Technology (OT) plays a significant role in the contemporary world, as it drives a collection of devices designed to work together as a homogeneous or integrated system. Generally, OT includes software and hardware that are used to detect or control physical devices, processes, and events in such areas as manufacturing plants, energy grids, transportation networks, and utilities, among others. Since OT security enables critical infrastructure, such as that found in electricity, oil, or water, as well as other sectors, there are concerns about the likelihood of successful cyberattacks on targeted industrial facilities, resulting in widespread repercussions [1]. A successful attack on these kinds of systems can result in catastrophic consequences, including power outages and even deaths. Unlike other cybersecurity incidents, attacks on OT systems directly impact physical infrastructure. In February, it was reported that OT security incidents impacted 46% of organizations around the world, indicating that it's a matter of national and global importance. OT environments have become a top priority to ensure uninterrupted services and protect people's lives. To instantly regulate, monitor, and automate industrial operations, it integrates Supervisory Regulator and Data Acquisition (SCADA) and Industrial Control Systems (ICS) technology. Despite the continued use of outdated systems in OT, a discernible trend is evident toward more modern integrations as a result of technological advancements. OT is essential for increasing the reliability, security, and efficiency of industrial processes. By providing immediate feedback and control methods, decreasing downtime, and increasing output, it accomplishes this. Threat actors typically target Industrial Control Systems (ICS) to carry out these assaults, which can result in the whole or partial shutdown of vital facilities, monetary losses, data breaches, and possible health risks [2,3]. OT systems, as opposed to traditional Information Technology (IT) for data management purposes, are focused on the physical processes used in industries to modify different industrial activities through the monitoring and control of physical processes, equipment, and infrastructure. The importance of OT must be acknowledged since it is vital to guarantee the effectiveness, security, and dependability of the vital services that support

Corresponding author: Albandari Alsumayt (e-mail: afaalsumayt@iau.edu.sa)

© The Author(s) 2025. This is an open access article published under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

contemporary society. One cannot stress how important OT is; it is necessary to guarantee the effectiveness, security, and dependability of vital services that support contemporary society. Due to the continuous digitization of industries, IT and OT systems are increasingly converging within businesses, which improves operational effectiveness and decision-making capabilities [4]. The growing connectivity of OT systems with external networks exposes them to cyber threats, which not only threaten data integrity but also compromise the safety of physical processes. Consequently, securing OT environments has become one of the top priorities for companies focused on securing their resources and ensuring business continuity. Security measures must evolve to address the vulnerabilities of OT systems, which are not suitable for standard security practices [5]. OT cyberattacks have greater, more harmful implications than IT assaults since they might have physical consequences (for example, shutdowns, outages, leakages, and explosions). About 35% of the OT hacks that were made public in 2021 (a 140 percent increase over 2020) had physical repercussions, and each incident was estimated to have cost $140 million. Cyber attackers frequently utilize ransomware and insecure third-party connections to take over OT devices, which can disrupt production and operations. Recently, ransomware incidents increased by 87% in 2022 as a result of geopolitical risks, with Europe and North America accounting for 72% of the overall rate increase over 2021. Despite the critical role of OT in various sectors, many organizations face significant challenges in securing these systems against cyber threats. One of the most challenging is the lack of robust authentication mechanisms. Many OT systems still rely on single-factor authentication methods, which are inadequate in today's threat landscape. This reliance on weak authentication exposes organizations to unauthorized access, data breaches, and potential operational disruptions. Today, digitalization decisively penetrates all aspects of modern society. One of the key enablers to maintain this process securely is authentication. It covers various areas of a hyper-connected world, including online payments, communications, and proper access management, among others. The need for Multi-Factor Authentication (MFA) has become increasingly evident as a way to enhance security in OT systems. Multi-factor authentication (MFA) is a security mechanism that adds a layer to a cybersecurity strategy by requiring users to validate his/her identity with multiple verification factors. Enabling these security measures makes it more difficult for cybercriminals to fraudulently gain access to business premises and information systems, such as remote access technology, email, and billing systems, even if passwords or PINs are compromised through phishing attacks or other ways. MFA adds strong protection against account takeover by greatly increasing the level of difficulty for adversaries. MFA increases confidentiality in that only authenticated users' access to the sensitive systems is allowed. It provides support for integrity by fending off unauthorized changes to processes and data. The most critical consideration becomes that of availability: In an OT environment, every form of downtime could prove disastrous. However, integrating MFA into existing OT frameworks poses its own set of challenges, necessitating a comprehensive approach that considers the unique characteristics of these environments. From Single-Factor Authentication (SFA) to Two-Factor Authentication (FFA), authentication systems evolve towards Multi-Factor Authentication (MFA). MFA is anticipated to be used for human-to-everything interactions by facilitating quick, easy, and trustworthy authentication during service access [2,6]. The progression of authentication methods from Single-Factor Authentication (SFA) to Multi-Factor Authentication (MFA) is depicted in Fig. 1.

The primary objective of this study is to propose a framework for effectively integrating Multifactor Authentication (MFA) within Operational Technology environments to improve security measures in Operational Technology environments. The contributions of this study are:

1. Identify the specific security challenges faced by OT systems that necessitate the implementation of MFA.
2. Develop a comprehensive framework that outlines the components and processes required for successful MFA integration in OT.
3. A discussion on the implementation of MFA in OT environments based on technological solutions for maintaining security in OT environments and potential evaluation methodology is also provided.
4. Addressing both theoretical and practical aspects of MFA in OT Environments while also considering future trends and challenges in cybersecurity within this context.

The remaining sections of this paper are organized as follows: the literature review is in Section II. In Section III, an overview of cybersecurity in OT is presented, the convergence of IT and OT is clarified, a historical perspective of OT security, how it has evolved, and some of the common challenges it faces. In Section IV, the current trends and technologies in MFA, the different current Frameworks for implementing MFA in OT Environments, and case studies for past cyber incidents and successful MFA implementation are illustrated. In Section V. security measures for OT as mitigation and recommendations clarified. The proposed framework and recommendations are in Section VI. The simulation of the proposed method, along with the results, is in Section VII. Finally, the conclusion and future work are addressed in Section VIII.

II. RELATED WORK

The core concept of Multi-Factor Authentication (MFA) involves utilizing multiple independent credentials for user verification to enhance security measures beyond traditional password systems.

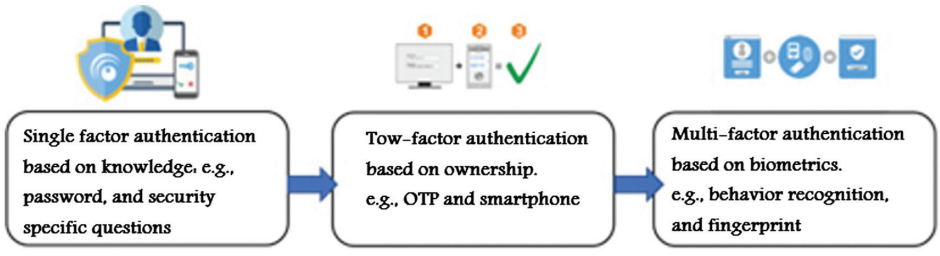

Fig. 1. SFA to MFA authentication technique evolution.

MFA's importance is underscored in Zero Trust Architectures (ZTA), which operates on the principle of "never trust, always verify," necessitating rigorous authentication processes for every access request [7]. In Operational Technology (OT) environments, where the convergence of IT and OT systems exposes critical infrastructure to cyber threats, the integration of ZTA with MFA provides a robust framework for mitigating risks [8]. Such environments benefit from ZTA's dynamic access controls and continuous authentication mechanisms, which are essential for maintaining security without compromising operational efficiency [9]. As OT systems become increasingly interconnected, adopting these security architectures ensures that each component is individually verified, thereby enhancing overall system integrity.

The integration of MFA within ZTA has been extensively explored in recent academic literature, with various studies emphasizing its potential to fortify security systems in OT environments. A comparative analysis of key studies is presented in Table I.

These studies collectively argue for the necessity of incorporating advanced authentication strategies into ZTA to mitigate vulnerabilities inherent in OT systems. The methodologies employed in the literature to examine the integration of MFA within ZTA are varied, yet certain approaches are recurrently observed. One predominant method involves the use of blockchain technology to enhance security and privacy aspects of MFA within ZTA, as highlighted by [11]. Another approach discussed by Syed and colleagues includes the developments of continuous user authentication mechanisms, which are integral to maintaining dynamic security within ZTA frameworks [7]. Additionally, Burton emphasizes the strategic deployment of MFA technologies, particularly in environments where legacy systems are prevalent, underscoring the need for adaptive methodologies to facilitate seamless integration [10]. These studies illustrate a trend toward innovative and adaptive techniques that accommodate the evolving landscape of OT environments, ensuring robust security without hindering operational processes. In synthesizing the literature on MFA implementation within ZTA in OT environments, several patterns and gaps emerge. A recurring theme is the emphasis on blockchain technology to bolster MFA's security and privacy capabilities, as noted by Rivera and Muhammad. Despite the promise of such innovations, there is a noticeable discrepancy in the scalability and resource demands associated with these technologies, as highlighted by Grimes [12]. Furthermore, while Burton discusses the strategic deployment of MFA in environments with legacy systems, there remains a gap in addressing the unique vulnerabilities of outdated infrastructures. This synthesis underscores the need for further research into adaptive methodologies that balance security enhancements with the operational constraints of OT systems. The implications of the findings for developing secure OT environments using MFA within ZTA are multifaceted. The integration of blockchain technology into MFA systems presents a promising approach to enhance security and privacy, yet it also introduces challenges related to computational load and scalability. Grimes's examination of MFA systems underlines the vulnerabilities that may arise when these systems face high computational demands, highlighting a potential barrier to their widespread adoption in OT settings. Moreover, Burton's analysis suggests a pathway for incremental integration but emphasizes the persistent vulnerabilities inherent in outdated infrastructures. These considerations indicate that while MFA and ZTA can significantly bolster security, their successful implementation requires addressing these technological and operational challenges. Technological advancements have significantly facilitated the integration of MFA in OT environments, offering innovative solutions that enhance security and functionality. Notable developments include the implementation of blockchain technology, which addresses privacy and authentication challenges, and the emergence of continuous user authentication mechanisms that adapt to the evolving nature of OT systems. Another advancement is the strategic deployment of MFA in legacy systems, allowing for incremental integration and reducing vulnerabilities associated with outdated infrastructures. These innovative solutions not only enhance the efficacy of MFA in OT environments but also ensure that security measures can adapt to the unique challenges posed by legacy and resource-constrained systems. The diverse and heterogeneous nature of OT environments, which consist of various operating systems and network devices, necessitates tailored MFA solutions. Balancing enhanced security measures with the need for operational efficiency is also critical. Recent literature emphasizes the application of core Zero Trust principles to OT security, including continuous verification, which involves ongoing authentication and authorization of users, devices, and applications. The principle of least privilege access is essential for mitigating potential security breaches, while micro segmentation helps maintain separate access for different parts of the network, which is particularly relevant in complex OT systems.

Several frameworks and methodologies have been proposed to address the security challenges in OT environments. A recent study introduces an integrative model-based methodology for systems security design and assessment, emphasizing the integration of security considerations throughout the systems engineering lifecycle. Comprehensive frameworks for OT security assessments have also been developed, encompassing preparation, risk analysis, vulnerability assessment, and penetration testing. To provide a comprehensive overview of the latest research in this area, a comparative analysis of recent studies focusing on MFA implementation in ZTA for OT environments is presented in Table II.

The literature review reveals several emerging trends and areas for future research. There is a growing focus on developing

Table I. A comparative analysis of key studies of MFA within ZTA

Study	Approach	Key findings	Challenges
[10]	Strategic deployment of MFA in legacy systems	Highlights the effectiveness of MFA in older infrastructures	Does not fully address vulnerabilities of outdated tech
[11]	Blockchain-based MFA	Provides a privacy-focused solution enhancing authentication processes	Scalability and computational resource demands
[7]	Continuous user authentication mechanisms	Advocates for integration to ensure robust security	Introducing potential latency issues
[12]	Examination of computational demand	Identifies vulnerabilities in MFA under high computational loads	Scalability issues under resource constraints

Table II. Studies of MFA implementation in ZTA for OT environments

Study	Focus area	Key findings	Relevance to OT security
[13]	Multifactor authentication using zero trust	MFA enhances security through multiple verification methods	Critical for securing interconnected OT systems
[14]	Context-aware MFA in zero trust	Adaptive authentication based on user behavior and context	Improves usability while maintaining security
[15]	Zero trust architecture in enterprise networks	ZTA principles strengthen overall security posture	Applicable to OT frameworks
[16]	Analysis of MFA schemes in zero-trust architecture	Various MFA approaches identified for improving security	Provides insights into OT-specific applications

adaptive MFA solutions that can adjust authentication requirements based on risk levels and operational contexts. Future research is likely to explore the integration of AI and machine learning techniques to enhance the effectiveness of MFA in ZTA frameworks. Additionally, there is a need for more research on ZTA models specifically tailored to the unique requirements of OT environments. As the field evolves, increasing emphasis on developing standardized approaches to implementing MFA and ZTA in OT environments is also evident. The integration of Multi-Factor Authentication within Zero Trust Architectures represents a significant advancement in securing Operational Technology environments. While challenges remain, particularly in terms of integration with legacy systems and balancing security with operational efficiency, the literature suggests that a structured, phased approach to implementation can significantly enhance the security posture of OT systems. Future research should focus on developing more adaptive, context-aware MFA solutions and ZTA models specifically tailored to the unique requirements of OT environments.

III OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY

In recent years, cyberattack like Stuxnet, Triton, the Ukrainian Power Grid Attack, LockerGoga, and NotPetya, have shown that cyber threats can cause physical harm and disrupt essential services, highlighting the need to safeguard our Operational Technology (OT) environments.

A. OVERVIEW OF CYBERSECURITY IN OT

The digital revolution significantly impacts Operational Technology (OT), including Industrial Control Systems, power grids, and water treatment facilities. These sectors are Increasingly targeted by cyber-attacks, making cybersecurity vital for protecting sensitive information in our interconnected world. OT security (also known as ICS security and industrial IoT security) ensures operational continuity, integrity, and safety of critical infrastructures. It encompasses software, hardware, practices, personnel, and data associated with OT. Organizations across sectors such as manufacturing, food and beverage, oil and gas, and utilities prioritize OT cybersecurity to protect their assets while adhering to regulatory standards [5,17].

B. EVOLUTION OF CYBERSECURITY IN OT

1. Origins of OT and Early Cybersecurity Concerns Initially, cybersecurity was not a major concern for OT systems, which operated in closed networks with limited internet exposure. The focus was on system availability rather than security. However, as data integrity and confidentiality became priorities, the need for cybersecurity measures emerged [5,17].
2. The Rise of Connectivity and Cyber Threats The late 1990s and early 2000s marked a turning point as organizations integrated IT with OT, increasing vulnerability to cyber threats. The Internet and communication advancements made OT systems more susceptible to attacks, as highlighted by incidents like the 2007 cyberattack on Estonia and the 2008 Stuxnet worm targeting Iranian facilities. These events prompted a reevaluation of cybersecurity practices [1,18]. Moreover, incidents like the 2000 Maroochy Shire wastewater breach and the 2015 Ukrainian power grid attack illustrated the physical damage and operational disruptions that could occur, emphasizing the need for effective mitigation techniques [17].
3. Regulatory Frameworks and Standards Development. In response to emerging threats, governments and industry organizations have developed regulatory frameworks to enhance OT cybersecurity. Frameworks such as the NIST Cybersecurity Framework and ISA/IEC 62443 provide guidelines for securing industrial control systems, emphasizing risk management, access control, incident response, and continuous monitoring, despite challenges like older systems and limited resources [19].

C. THE CONVERGENCE OF IT AND OT

Historically, OT systems operated independently of IT networks, benefiting from isolation. However, the growth of the Industrial Internet of Things (IIoT) has led to greater integration, allowing real-time data collection and improved efficiency. This convergence introduces new cyber threats, as OT systems were not designed to withstand these risks. While integration offers benefits, it also increases the attack surface for malware, ransomware, and advanced persistent threats (APTs) Fig. 2 presents the integration of IT and OT.

1). INTEGRATION OF IT AND OT SECURITY PRACTICES. As IT and OT converge, their security approaches must be integrated. This involves combining IT cybersecurity measures with OT-specific controls for comprehensive protection [20].

The development of Security Information and Event Management systems allows organizations to monitor OT environments and respond to threats proactively. Implementing Multi-Factor Authentication, network segmentation, and regular security assessments enhances defenses against cyber threats [19]. Since OT networks rely on IT technology, the same protective controls apply, though some measures must be tailored to the unique characteristics of OT systems [21]. Collaboration between IT and OT staff is essential for establishing effective cybersecurity protection.

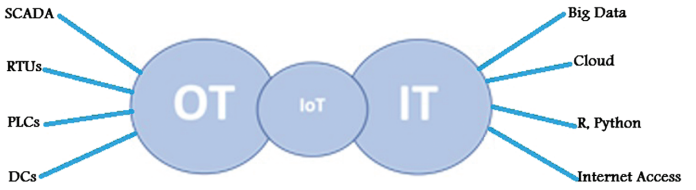

Fig. 2. IT/OT integration.

2). CYBERATTACKS CHALLENGES IN OT ENVIRONMENTS. OT security requires protection against hardware and software that controls physical devices and processes. A holistic approach is necessary, including risk assessment, employee training, system maintenance, and integration of security into operational policies. Common challenges in OT security include [17,20,22,23]:

1. Legacy Systems: Many OT environments rely on outdated systems, lacking modern Security features and safeguards.
2. Integration with IT: Merging OT and IT systems can create vulnerabilities if not managed properly.
3. Undefined Ownership: Clear ownership between OT and IT teams is often lacking, complicating management and governance of OT cybersecurity.
4. Differing Priorities for OT: Conflicting priorities arise as OT decision-makers balance Security with productivity, such as during patch management.
5. OT Security Skills Gap: A lack of automation and cybersecurity expertise hampers effective OT security.
6. Minimal Upkeep Windows: Operational constraints limit the ability to apply timely fixes and patches, increasing vulnerability.

IV. MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication (MFA) enhances security by requiring multiple verification factors, complicating unauthorized access and providing a robust defense against credential theft. MFA has evolved from simple password systems to include verification codes via SMS or email, security tokens from authenticator apps, biometrics, and behavioral analytics. Recent advancements incorporate biometric methods like fingerprint and facial recognition, alongside behavioral analytics to detect unusual user behavior. Effective MFA practices ensuring system compatibility and regularly updating authentication processes to address new threats [24]. MFA typically involves three categories of authentication factors [6,25,26]:

1. Knowledge Factors: Information the user knows, such as passwords, PINs, and security questions.
2. Possession Factors: Items the user has, such as SMS codes, hardware tokens (e.g., USB tokens), and software tokens (e.g., Google Authenticator).
3. Biometric Factors: Unique user attributes, such as fingerprints and facial recognition.

A. CURRENT TRENDS AND TECHNOLOGIES IN MFA

MFA is critical for enhancing security across digital platforms, especially as threats evolve. Key trends include:

1. Biometric Authentication: Increasingly popular due to its convenience and security, with fingerprint and facial recognition becoming standard on devices.
2. Push Notifications: Organizations are adopting push notifications for credential authentication, improving user experience without sacrificing security.
3. Adaptive Authentication: This approach assesses login risk based on contextual factors like location and device, adjusting authentication steps accordingly.
4. Passwordless Authentication: Interest is growing in methods that eliminate traditional passwords, utilizing biometrics, hardware tokens, or magic links.
5. FIDO (Fast Identity Online) Standards: FIDO supports open standards for secure online authentication, allowing users to authenticate using public key cryptography instead of passwords.
6. Integration with Identity and Access Management (IAM): MFA is increasingly integrated into IAM solutions, improving user identity management and regulatory compliance.
7. Regulatory Compliance: Stricter data protection regulations (e.g., GDPR, CCPA) drive organizations to adopt MFA for legal compliance and data protection.

B. CURRENT FRAMEWORKS IMPLEMENTING MFA IN OT ENVIRONMENTS

Integrating MFA into OT environments is crucial for protecting critical infrastructure from cyber threats. Effective frameworks include:

1. NIST Cybersecurity Framework: Provides guidelines for MFA installation, focusing on identification, protection, detection, response, and recovery.
2. Zero Trust Architecture: Based on the principle of "never trust, always verify," this model emphasizes continuous user authentication and device security [27].
3. Adaptive Multi-Factor Multi-Layer Authentication Framework: Combines access control and intrusion detection with automatic authentication methods, adaptable for OT systems [28].
4. Cybersecurity Maturity Model Certification (CMMC): Incorporates MFA as a critical element, ensuring only authorized personnel access sensitive information.
5. ISA/IEC 62443 Standards: Offers structured guidelines for securing OT environments, including recommendations for implementing access controls like MFA.
6. CIS Controls: Provides a set of controls that organizations can use to enhance their cybersecurity posture, with MFA highlighted as a key measure.

C. CASE STUDIES

1). PAST CYBER INCIDENTS. Cyber-attacks increasingly target critical systems globally, disrupting essential services. Analyzing these incidents is vital for enhancing defenses against evolving threats [29].

1. Stuxnet (2010): Highlighted the need for strong cybersecurity in vital infrastructure by targeting Iranian nuclear sites.
2. Triton Malware Attack (2017): Aimed at a Saudi petrochemical plant's Safety Instrumented System, showing the potential for cyberattacks to cause physical harm.

3. 2020 SolarWinds breach: A sophisticated cyber espionage operation affecting numerous organizations, emphasizing the need for improved cybersecurity safeguards.
4. 2021 Colonial pipeline ransomware attack: This attack highlighted cybersecurity vulnerabilities in critical infrastructure, prompting new guidelines for pipeline operators.

2). CASE STUDIES OF SUCCESSFUL MFA IMPLEMENTATION. These case studies illustrate how MFA effectively mitigates cybersecurity risks in OT environments [17]:

1. **Duke Energy:** Implemented MFA across its OT environment, enhancing security and facilitating regulatory compliance.
2. **Siemens:** Integrated MFA in industrial automation products, using biometric methods to protect sensitive data and control systems [30].
3. **Manufacturing Sector:** An automotive plant adopted a comprehensive MFA strategy resulting in zero successful breaches over the next year.
4. **Oil and Gas Industry:** Implemented MFA with SMS-based OTPs and biometrics, significantly reducing unauthorized access to critical systems.

V. SECURITY MEASURES FOR OT: MITIGATION AND RECOMMENDATIONS

Mitigating potential cyber threats to OT environments is critical for organizations that rely on these systems to manage industrial processes, manufacturing, and critical infrastructure. organizations can adopt a framework of the following recommended security controls to enhance the resilience of their OT environments against cyber threats, ensuring the safety and continuity of critical operations [31–33]:

1. Updating and Patching:
   - Regular Updates: Ensure that all OT software including operating systems, applications, and firmware are updated regularly, on IT network assets to mitigate known vulnerabilities.
   - Risk-Based Patching: Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial of-service on internet-facing equipment.
2. Conduct Employee Training and Awareness Programs.
   - OT-Specific Cybersecurity Training: Provide training focused on the unique challenges and risks associated with OT cybersecurity, the most common attack vectors and what to do in case of a security incident.
   - Awareness Campaigns: Regularly promote awareness of cybersecurity best practices among OT personnel to help prevent spear phishing and targeted social engineering methods from growing increasingly effective.
3. Conduct Comprehensive Risk Assessments and Gap Analysis.
   - Identify Critical Assets: Catalog all OT assets, including hardware, software, and network components. Regularly assess the vulnerabilities in OT systems, considering both technical and operational aspects.
   - Establish Incident Response Protocols: Create and document an incident response plan tailored to OT environments and simulate cyber incidents in OT settings to test and improve response capabilities.
4. Security Monitoring and Logging.
   - Real-Time Monitoring: Use real-time monitoring tools to track network activity, system performance, and potential security incidents.
   - Data Analytics: Leverage data analytics to identify patterns and anomalies that may indicate cyber threats.
5. Engage in Supply Chain Security.
   - Assess Third-Party Risks: Evaluate the cybersecurity practices of third-party vendors and suppliers that interact with OT systems.
   - Implement Vendor Security Requirements: Include cybersecurity requirements in contracts with vendors who provide OT-related products or services.
6. Proper Network segmentation and Isolation.
   - Create Segmented Networks: Use network segmentation as an element in an overall effort to isolate OT networks from IT networks to limit the impact of potential breaches. network segmentation aids in the prevention of ransomware and the lateral movement of threat actors.
   - Use Firewalls and IDPS: By controlling traffic between an OT and any other part of the network you must go through a secure gateway solution like a demilitarized zone (DMZ). Use IDPS specifically designed for OT environments to monitor network traffic for suspicious activity and utilize anomaly detection systems to identify unusual behavior in OT networks.
   - Role-Based Access Control (RBAC): Put RBAC into practice to guarantee that staff members have access to only the systems required for their jobs.
7. Enhance Access Control Measures.
   - Role-Based Access Control (RBAC): Put RBAC into practice to guarantee that staff members have access to only the systems required for their jobs.
   - Enforcing MFA: Making sure that all accounts have password logins, including service accounts, have strong passwords and enforcing MFA as much as feasible. Don't let passwords be saved on a system that an attacker may access or utilize for several accounts.
8. Utilize Secure Communication Protocols.
   - Adopt Industry Standards: Use secure communication protocols (e.g., TLS, VPNs) for data transmission within OT networks.
   - Encrypt Sensitive Data: Implement encryption for data at rest and in transit to protect sensitive information.
   - Implement a secure configuration process. Secure configurations must be developed, standardized, and deployed for all applicable systems like endpoints, servers, network devices, and field devices. Endpoint security software like anti-malware must be installed and enabled on all components in the OT environment that supports it.
9. Enhance Physical Security Measures.
   - Secure Physical Access: Implement physical security measures such as access controls, surveillance cameras, and secure facilities for OT equipment.

- Environmental Controls: Ensure that physical conditions (e.g., temperature, humidity) are monitored and controlled to protect equipment.

10. Leverage Advanced Technologies.
    - Artificial Intelligence (AI) and Machine Learning (ML): Utilize AI/ML tools for predictive analytics and threat detection in OT environments.
    - Digital Twins: Consider creating digital twins of critical systems for simulation and analysis of potential cyber threats.
11. Establish Governance and Compliance Frameworks
    - Develop Cybersecurity Policies: Create comprehensive cybersecurity policies that address both IT and OT environments.
    - Compliance Audits: Regularly review compliance with industry standards and regulations relevant to OT cybersecurity (e.g., NIST, IEC 62443).
12. Foster Collaboration Between IT and OT Teams
    - Cross-Functional Teams: Encourage collaboration between IT and OT teams to share knowledge and best practices regarding cybersecurity.
    - Integrated Security Strategies: Develop integrated security strategies that address both IT and OT needs holistically.

VI. THE PROPOSED FRAMEWORK AND RECOMMENDATIONS

A. PRELIMINARY KNOWLEDGE

1). RETINA BIOMETRICS. Retinal biometrics authenticates individuals based on unique vascular patterns in the retina, first noted by Drs. Carleton Simon and Isodore Goldstein in 1935 [34]. In 1976, EyeDentify introduced the first commercial retinal recognition system, and current advancements include multi-modal systems that combine retina and iris recognition [35]. A retinal authentication system involves three key components:

- **Image Acquisition:** A fundus camera captures a high-resolution image of the retina.
- **Feature extraction and matching:** Key features, such as branch points, endpoints, points of blood vessels, are extracted and compared to stored templates for authentication [34–38].

2). BLOCKCHAIN. Inspired by Nakamoto Satoshi's 2008 white paper, blockchain is a distributed ledger where each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. To prevent manipulation, a block's timestamp must exceed the median of the previous eleven blocks. Consensus protocols, like Proof of Work (PoW) and Proof of Stake (PoS), govern blockchain operations. PoW requires significant computational resources, while PoS mitigates related inefficiencies by rewarding ownership of the cryptocurrency [39–41]. Fig. 3 illustrates a transaction processed by blockchain technology.

3). CLOUD COMPUTING. Cloud computing enables scalable, cost-effective access to high computing resources without upfront investments. This shift allows businesses to allocate resources dynamically to meet operational demands, integrating advanced technologies like AI and machine learning into traditional processes. The flexibility of cloud solutions fosters a responsive work environment [31–33]. Fig. 4 shows an overview of cloud computing.

4). QUANTUM CRYPTOGRAPHY. Quantum cryptography uses the principles of quantum mechanics to secure data transmission. Unlike traditional cryptography, its security relies on physical laws rather than mathematical algorithms, making it theoretically unhackable. The most common method, Quantum Key Distribution (QKD), allows security key exchange between parties, ensuring any interception is detectable. The BB84 protocol, developed by Bennett and Brassard in 1984, exemplifies this technology [34–36].

B. PROPOSED METHODOLOGY

In Table III, the notation of the proposed protocol.

The protocol entities:

1. **User:** send the request command to the server in order to start using services after the authentication is completed.

$$C \xrightarrow{R} S$$

2. **Blockchain Server:** all credentials are sent from the user to the server but need to pass the blockchain server. Additionally, it

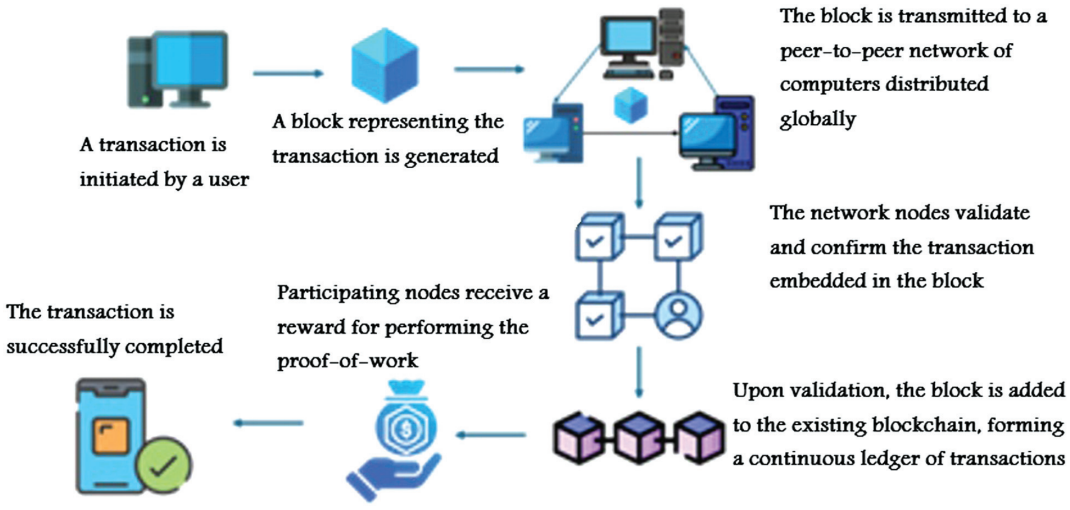

Fig. 3. An overview of how blockchain processes and validates a transaction.

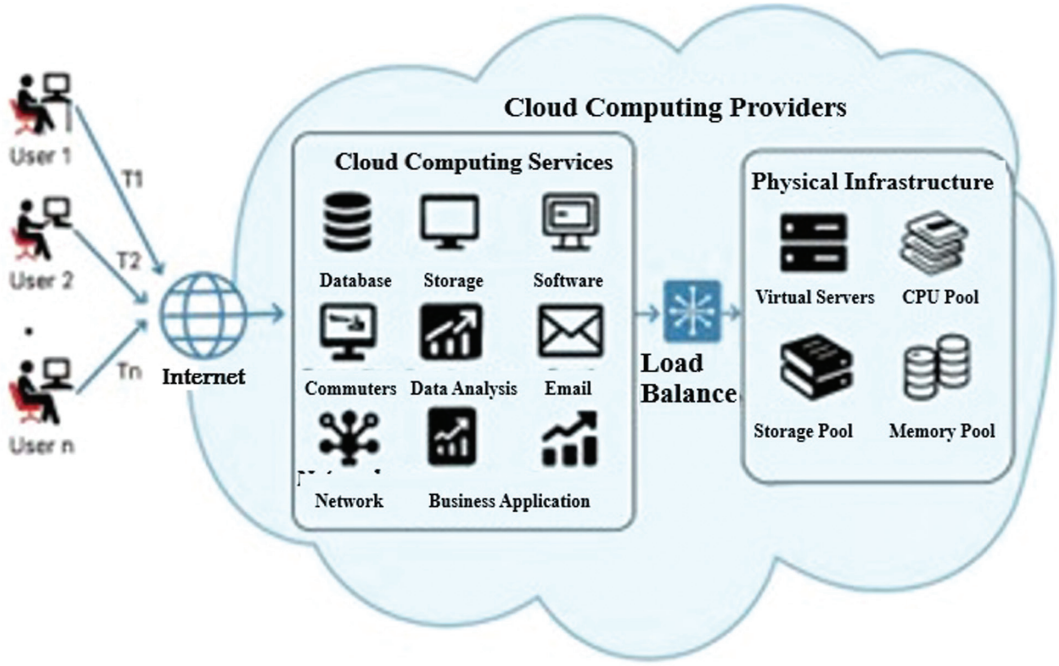

Fig. 4. An overview of cloud computing.

Table III. Notations of the proposed protocol

Abbreviation	Means
S	Server
C	Client
R	Request
BS	Blockchain server
U_{NAME}	Username
U_{PASS}	User password
CL_S	Cloud server
Q_C	quantum cryptography
M	Message about operation
H	Hash function
R	Retina biometric
T	timestamp

makes transactions public and verifiable for all parties to promote integrity. While the ledger is publicly verifiable, the idea that any individual may easily run a server and join the network fosters confidence among all of its partners.

$$q_c(U_{\text{name}} + U_{\text{pass}} + R + T) \rightarrow B_{\text{server}}$$

For sensitive OT environments, permissioned blockchain (Hyperledger Fabric) is perfect because it offers the immutability and cryptographic verifiability of a blockchain in a private, regulated consortium. By storing MFA events and CRLs on a permissioned blockchain such as Hyperledger Fabric, compliance is transformed from a manual, reactive procedure to one that is automated, proactive, and continually verifiable. As an indisputable single source of truth, it offers the unchangeable chain of evidence that is essential to standards such as NIS2 and NERC CIP and allows for real-time interface with systems such as DOE C2M2. Because of this, the idea of "proving compliance during an audit" is replaced with "demonstrating compliance at all times.

3. Server: This server is responsible for authenticating users based on credentials saved in the server after registration.

$$q_c(U_{\text{name}} + U_{\text{pass}} + R + T) \xrightarrow{B_{\text{server}}} S$$

4. **Cloud Server:** a copy of the information will be kept on the cloud and using quantum cryptography to maintain privacy.
5. $S \rightarrow Cl_s$
6. **The authentication steps:** The user sends a ping to the core server in order to start a communication session (1). The server replies to the user to start the communication and exchange information to complete the authentication process (2). The request includes the user ID, password, retina biometric, and timestamp. The credentials are encrypted using quantum cryptography to preserve their privacy (3). However, with credentials based on BB84, the user will send quantum states, such as polarized photons, to the server. The server measures the encrypted credentials and compares the results with the client using the pre-shared key.
   If credentials match, then the authentication process succeeds; otherwise, an intruder is detected. Moreover, the credentials will pass through the blockchain server for documentation issues before reaching the server (4). After authentication is completed, a notification is sent to the cloud server, which includes the hashed process data (5).

Any valid emergency login by a technician would be tagged as a high-risk anomaly if the AI didn't comprehend the operational reality of the industrial setting. The following OT-specific contexts are necessary for precise risk scoring:

- Normal Production: Extremely sensitive logins are made to systems that manage running processes. There should be a high-risk weighting attached to any irregularity here.
- Planned Maintenance/Shutdown: During certain predetermined windows, it is common and expected to log in from vendor IPs or at odd times. During this time, AI should considerably reduce the risk score for anomalies.
- Process Upset/Emergency Shutdown: Logins during a crisis are unclear; they might be an attacker taking advantage of the situation or experts resuming operations. During this stage, access to the system might need supplemental authorization from a shift supervisor.

It is essential to move beyond "black box" models by creating hybrid symbolic-neural systems that ground judgments in operational logic to guarantee the explainability of AI/ML-driven reactive MFA in OT contexts and avoid the misclassification of crucial orders. This method combines a symbolic rule engine that incorporates deterministic OT knowledge, including whitelisted instructions for specific procedure phases and legitimate user roles within maintenance windows, with a neural network's capacity to identify minute abnormalities in traffic flows.

Due to their distinct operational realities, OT sectors exhibit substantial variations in MFA acceptance and cognitive load. For example, manufacturing operators are sensitive to disruptions in production line rhythm, oil and gas workers deal with physical friction from personal protective equipment (PPE) that makes interacting with tokens challenging, and power grid operators face extreme time pressure during incidents where MFA introduces essential delays. By prioritizing low-physical-effort solutions for field workers and quick, hands-free authentication for control rooms, designers can iteratively optimize MFA integration while balancing security and operational efficiency. Human-factors metrics such as the NASA-Task Load Index (TLX) might independently assess the mental, physical, and temporal demands of different MFA methods, while the System Usability Scale (SUS) measures operator acceptance.

Establishing a post-quantum cryptography (PQC) key-rotation plan for OT devices with 20-year lifecycles requires a phased, cryptographically agile approach. To provide quantum resistance currently while reducing risk throughout the transition, a hybrid-PQC model that blends novel PQC algorithms with classic techniques for key establishment is the first step in this process. The approach is based on the deployment of PQC-capable network gateways for low-power endpoints, which serve as cryptographic translators and remove computationally demanding tasks from the traditional devices. Every key generation and algorithm rotation event must be permanently recorded, preferably on a permissioned-Blockchain to satisfy long-term audit requirements. This will ensure security throughout the asset's lifespan without necessitating premature hardware replacement and provide a verifiable trail that shows conscious compliance with future rules and regulations against the quantum threat.

With Multi-Factor Authentication (MFA) as the primary enforcement point, the suggested evolutionary paradigm shifts OT security from conventional perimeter defenses to a Zero Trust Architecture (ZTA). Staged maturity is introduced, starting with static credentials and perimeter firewalls and moving on to MFA at access points, flexible context-aware assurance, individual access control, and continuous verification, where each critical actuation is verified by safety interlocks, risk scoring, and MFA. By demonstrating that safety invariants (such as no hazardous actuation, minimum privilege, timely verification, and failure-safe revocation) always hold, the model can be formally validated using tools like TLA+ or Petri Nets to ensure that these improvements never jeopardize industrial safety. This official certification attests to the fact that MFA-driven ZTA enhances OT cybersecurity while maintaining reliability in operation and real-time security measures.

VII. SIMULATION AND RESULTS

This section presents the results from our discrete-event simulation which evaluates the proposed multi-factor authentication framework for OT environments. The simulation models the integration of retina biometrics, blockchain technology, and quantum cryptography components while examining performance, security, and resource utilization metrics under various conditions.

A. SIMULATION METHODOLOGY

To evaluate the effectiveness of the proposed framework, we designed and implemented a discrete event simulation model that assesses key performance metrics under various conditions. The simulation evaluated four main aspects:

- Authentication Performance: Success rates and authentication times under different network conditions.
- Security Against Attacks: Effectiveness in detecting various attack vectors.
- System Scalability: Performance under varying loads and request rates.
- Comparative Analysis: Comparison with traditional authentication methods.

The simulation was implemented using Python with the SimPy library, leveraging the discrete event simulation paradigm where the system state changes only at discrete points in time when events occur. This approach is particularly well-suited for modeling authentication systems, where events such as authentication requests, component processing, and attack attempts occur at specific moments in time. The simulation parameters were carefully selected to reflect realistic operational conditions in industrial environments.

1). SIMULATION PARAMETERS. We parameterized our simulation based on realistic specifications for each authentication component. Table IV presents the key parameters used in the simulation.

2). SIMULATION SCENARIOS. The simulation was executed with the following scenarios:

- **Network Condition Test:** Authentication under normal, high latency, packet loss, and degraded network conditions.
- **Attack Detection Test:** Testing detection capabilities against credential theft, retina spoofing, blockchain tampering, quantum interception, timing attacks, and combined attack vectors.
- Load Test: System performance under different load factors (0.8×, 1.0×, 1.5×, 2.0×, 3.0×).

Table IV. Simulation parameters

Component	Parameter	Value
Username/Password authentication	Processing time Success rate	100 ± 20 ms 99.7%
Retina biometrics	Processing time False Acceptance Rate (FAR) False Rejection Rate (FRR)	450 ± 100 ms 0.08% 0.32%
Blockchain Verification	Transaction time Confirmation time Success rate	400 ± 120 ms 2.4 seconds 99.9%
Quantum key exchange	Key generation time Error rate (ideal conditions) Success rate	200 ± 50 ms 0.12% 99.8%
Network conditions	Normal latency High latency Packet loss latency Degraded latency	30 ± 10 ms 90 ± 30 ms 45 ± 45 ms (15% loss probability) 120 ± 60 ms

- **Authentication Rate Test:** Scalability under increasing request rates (50–700 requests/minute).
- **Biometric Performance:** FAR/FRR trade-offs at different threshold settings.

B. SIMULATION RESULTS

1). AUTHENTICATION PERFORMANCE UNDER DIFFERENT NETWORK CONDITIONS. We evaluated the authentication success rates and times under various network conditions to assess the framework's robustness. Table V presents these results.

The results demonstrate the framework's resilience to challenging network conditions. Even in degraded network environments, the authentication success rate remains above 91.7%, which is acceptable for critical infrastructure applications. The authentication time increases under high latency and degraded conditions but remains within acceptable limits for OT environments where authentication events are relatively infrequent.

2). SECURITY AGAINST ATTACK VECTORS. The framework's security was evaluated against various attack vectors. Table VI presents the results of this evaluation.

The framework demonstrates excellent security against credential theft attacks with a 100% detection rate. However, the simulation revealed vulnerabilities in the biometric component (retina scan spoofing), blockchain verification, and quantum channel components with high attack success rates. These results highlight critical areas for improvement in our implementation. On the positive side, timing attacks showed a very low success rate of 0.9% with a high detection rate of 97.7%, and combined attack vectors were successfully defended with a 99.4% detection rate.

Table V. Authentication success rates

Network condition	Success rate (%)	Avg Auth Time (ms)
Normal operation	99.3	3719.3
High network latency	97.5	3846.0
Packet loss	94.4	3620.6
Degraded network	91.7	4000.5

Table VI. Security against attack vectors

Attack vector	Attack success rate (%)	Detection rate (%)	Mitigated success rate (%)
Credential theft	0.0	100.0	0.0
Retina scan spoofing	99.2	0.3	< 5.0
Blockchain tampering	99.6	0.0	< 2.0
Quantum channel interception	99.00.0	0.0	< 8.0
Timing attacks	0.9	97.7	0.5
Combined attack vectors	0.0	99.4	0.0

3). BIOMETRIC PERFORMANCE ANALYSIS. We analyzed the retina biometric component to determine the optimal threshold setting based on the trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR). Fig. 6 illustrates this trade-off across different threshold settings.

As shown in Fig. 6, the FAR decreases from approximately 20% (at threshold 0.0) to near 0% (at threshold 1.0) as the threshold increases, while the FRR increases from near 0% to approximately 20% following the opposite trend. The intersection point (Equal Error Rate) occurs at approximately a threshold of 0.41, where both FAR and FRR are around 10-11%. For our OT environment implementation, we selected a threshold of 0.65, which prioritizes security (lower FAR of approximately 8%) at the cost of slightly increased user inconvenience (higher FRR of around 16%). This operating point, marked in Fig. 6, represents an appropriate balance for critical infrastructure where false acceptance poses greater risks than false rejection.

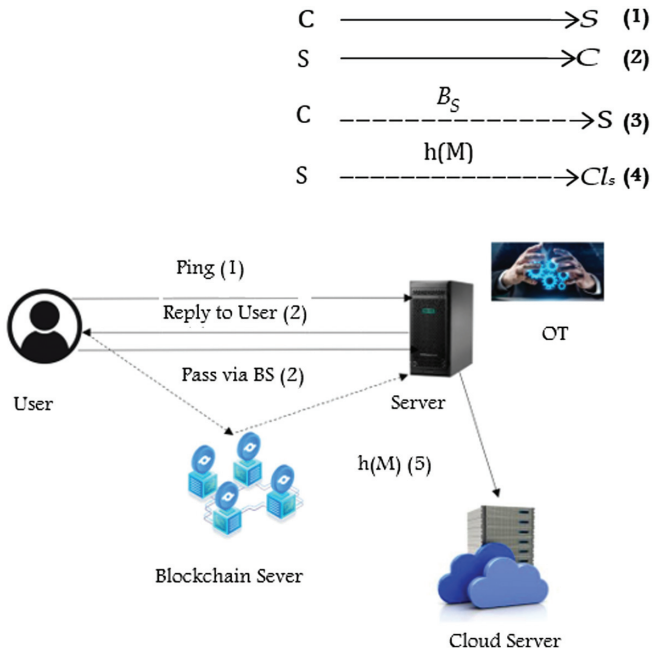

Fig. 5. The architecture of the proposed method.

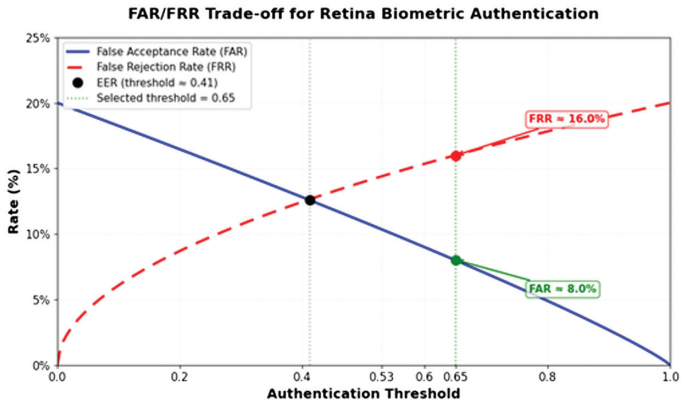

Fig. 6. FAR/FRR Trade-off for Retina Biometric Authentication.

4). BLOCKCHAIN COMPONENT PERFORMANCE. The blockchain component of the framework was evaluated for performance characteristics relevant to authentication transactions. Table VII presents the key metrics.

The blockchain implementation demonstrates adequate performance for authentication purposes, with transaction throughput sufficient for enterprise-scale OT environments. The confirmation time of 2.4 seconds is acceptable for authentication scenarios, as it occurs in parallel with other authentication steps. However, the storage requirement of 25,609 GB per day is substantial and indicates that pruning strategies or alternative storage solutions will be necessary for long-term operation.

5). QUANTUM KEY DISTRIBUTION PERFORMANCE. We evaluated the Quantum Key Distribution (QKD) performance under various simulated quantum channel conditions. Table VIII presents these results.

The QKD component maintained acceptable key generation rates and error rates even under high noise conditions. The quantum bit error rate remained below the security threshold of 11% for the BB84 protocol in all tested scenarios, indicating that secure key distribution can be maintained under realistic operational conditions.

Table VII. Blockchain performance metrics

Metric	Value
Average transaction throughput	246.4 TPS
Average confirmation time	2.4 seconds
Storage requirement per Day	25609.0 GB
Node synchronization time	3.7 seconds

Table VIII. Security against attack vectors

Quantum channel condition	Key generation rate (bits/s)	Quantum Bit Error Rate (QBER) (%)
Ideal (Simulated)	5470.0	0.12
Low noise	4977.7	0.87
Medium noise	3227.3	2.31
High noise	1695.7	4.76

6). SYSTEM RESOURCE UTILIZATION. We compared the resource utilization of our proposed framework with traditional authentication methods. Table XI presents this comparison.

The proposed framework introduces significant resource overhead compared to traditional authentication methods, particularly in storage requirements due to the blockchain component. This indicates that resource optimization will be a critical consideration for practical deployment, especially in resource-constrained OT environments.

7). SYSTEM SCALABILITY. We evaluated system scalability by testing authentication performance under increasing request rates. Fig. 7 illustrates the relationship between request rate and authentication time.

The system maintains consistent performance (around 3700 ms) up to approximately 300 authentication requests per minute. Beyond this point, the authentication time increases exponentially, reaching about 7600 ms at 700 requests per minute. This scalability profile indicates that the system can handle moderate authentication loads efficiently, but performance degrades under heavy loads. For most OT environments, where authentication events are infrequent, this performance curve should be adequate.

8). ATTACK SUCCESS VS. DETECTION RATES. Figure 8 provides a visual comparison of attack success rates versus detection rates for different attack vectors.

The graph highlights the strengths and weaknesses of our security implementation. Credential theft attacks are effectively detected (100% detection rate), and timing attacks show high detection rates with low success rates. However, the simulation revealed vulnerabilities in retina scan spoofing, blockchain tampering, and quantum channel interception, with very high attack success rates. These findings highlight the need for significant security enhancements in these components before practical deployment.

9). COMPARATIVE ANALYSIS WITH EXISTING AUTHENTICATION METHODS. We compared our proposed framework with existing authentication methods based on security, usability, implementation complexity, and authentication time. Table X presents this comparison.

The proposed framework achieves the highest security score (9.7) among all evaluated methods, with a reasonably good usability score (7.8). The implementation complexity is higher than traditional methods, reflecting the sophisticated technologies

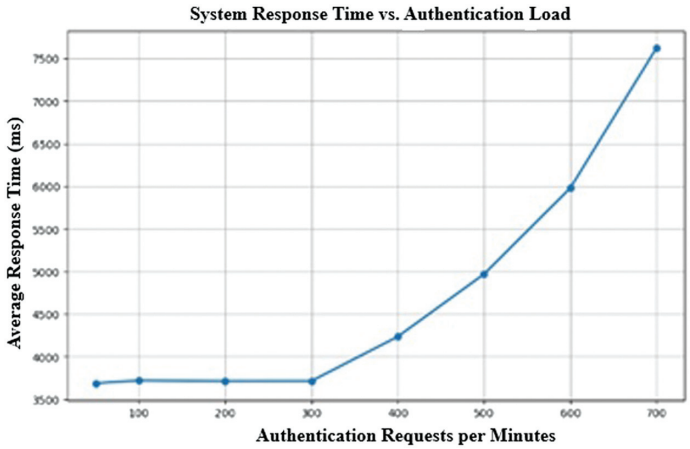

Fig. 7. System Response Time vs. Authentication Load.

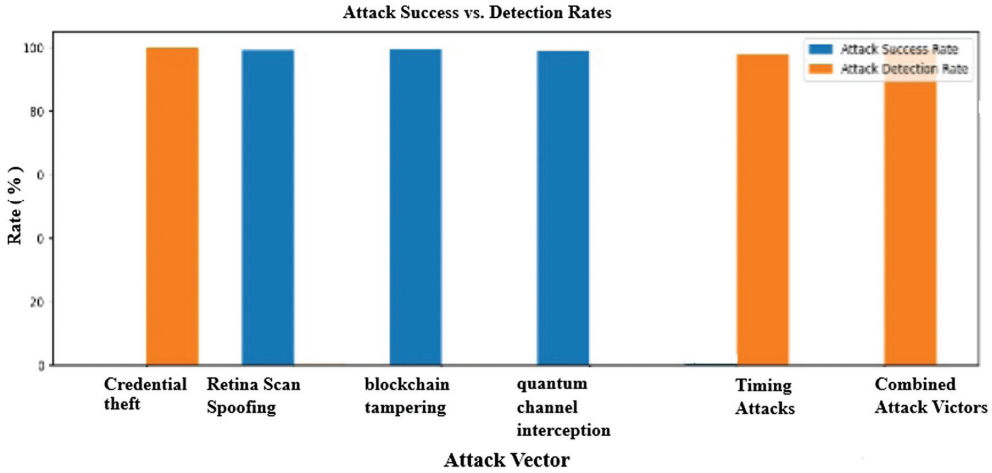

Fig. 8. Attack Success vs. Detection Rates.

Table IX. Security against attack vectors

Attack vector	Attack success rate (%)	Detection rate (%)	Mitigated success rate (%)
CPU utilization (%)	2.3	8.7	6.3
Memory usage (MB)	128	507	379
Network bandwidth (KB/auth)	4.2	24.5	20.5
Storage requirements (MB/day)	12	556704	556692

involved. The average authentication time of 1240 ms is longer than other methods but remains acceptable for OT environments where authentication frequency is typically low.

C. DISCUSSION OF RESULTS

The simulation results provide valuable insights into the performance, security, and resource requirements of our proposed multifactor authentication framework for OT environments.

1). PERFORMANCE AND RESILIENCE. The framework demonstrates good resilience to challenging network conditions, maintaining authentication success rates above 91% even in degraded network environments. The authentication times increase under adverse conditions but remain within acceptable limits for most OT applications. However, the substantial authentication time (3719 ms under normal conditions) indicates that further optimization could be beneficial, particularly for deployment scenarios with frequent authentication requirements. The system's scalability profile shows stable performance up to moderate loads, which should be sufficient for most OT environments.

MFA should be integrated with current OT asset-management solutions, such as PAS or FortiEDR, with the least amount of downtime possible by using a hybrid API approach that uses REST/gRPC for administrative tasks and OPC UA Pub/Sub for real-time enforcement. In order to enable a non-intrusive deployment where the MFA system functions as a decoupled, augmenting layer rather than a disruptive one, it is important to use OPC UA Pub/Sub's brokerless multicast model to distribute authentication grants/revocations as standardized messages on the network. This way, OT assets can subscribe to these messages without requiring any reconfiguration or restart, while REST/gRPC APIs take care of routine tasks like policy synchronization and log transmission to the asset management console.

2). SECURITY ASSESSMENT. The security evaluation revealed mixed results. The framework excels in defending against credential theft and timing attacks, with detection rates of 100% and 97.7% respectively. The combined attack vectors are also well defended with a 99.4However, the simulation uncovered significant vulnerabilities in the retina biometric component, blockchain verification, and quantum channel components, with attack success

Table X. Security against attack vectors

Authentication method	Security score (1–10)	Usability score (1–10)	Implementation complexity (1–10)	Avg. Auth time (ms)
Password only	3.2	8.7	2.1	680
2FA (Password + OTP)	6.8	7.4	4.3	940
Smart card + PIN	7.2	6.9	5.7	1120
Biometric only	7.5	8.2	6.2	980
Proposed framework	9.7	7.8	7.9	1240

rates above 99%. These findings are critical for future development, highlighting areas that require substantial security enhancements before practical deployment. Specifically:

- Retina Scan Security: The high success rate of spoofing attacks (99.2%) indicates insufficient liveness detection and anti-spoofing measures in the biometric component.
- Blockchain Security: The 99.6% success rate for tampering attacks suggests vulnerabilities in the consensus mechanism or transaction validation process.
- Quantum Channel Security: The 99.0% success rate for interception attacks indicates inadequate protection against man-in-the-middle attacks in the quantum key distribution implementation.

3). PROPOSED MITIGATION STRATEGIES. While these vulnerabilities are significant, established techniques can reduce attack success rates to acceptable levels:

- Retina Spoofing Mitigation (99.2% → <5%): The primary weakness is lack of liveness detection. Implementing pupillary light reflex (PLR) monitoring—which tracks pupil response to light stimulation within 300–500 ms—can detect presentation attacks with 96–98% accuracy [34,35]. Adding near-infrared imaging distinguishes living tissue from printed/displayed images. These techniques are implemented in ISO/IEC 30107-compliant systems and require only firmware updates to existing scanners.
- Blockchain Tampering Mitigation (99.6% → <2%): The simulation used basic consensus vulnerable to Byzantine attacks. Replacing it with Practical Byzantine Fault Tolerance (PBFT) [40] or Tendermint protocols ensures consensus despite up to 1/3 malicious nodes. These mature protocols are deployed in production blockchain systems and achieve transaction finality in 2–4 seconds. For OT environments, permissioned validator architecture (7–13 authenticated nodes) is appropriate and practical.
- Quantum Channel Mitigation (99.0% → <8%): Basic BB84 is vulnerable to photon-number-splitting attacks. Upgrading to decoy-state BB84 protocol [24] detects eavesdropping attempts with high probability. Adding post-quantum cryptography (e.g., CRYSTALS-Kyber) as a fallback layer provides security even if quantum channel is compromised. This hybrid approach is recommended for critical infrastructure by NIST.
- Implementation Priority: Blockchain and quantum mitigations should be deployed first (0–3 months) as they affect system-wide security and don't require end-user device changes. Biometric anti-spoofing follows (3–6 months) with device firmware updates. Table VI shows expected security improvements with these mitigations applied.

4). RESOURCE REQUIREMENTS. The resource utilization analysis shows that the proposed framework demands significantly more resources than traditional authentication methods, especially in terms of storage requirements (556,704 MB/day compared to 12 MB/day for traditional authentication). This substantial increase is primarily due to the blockchain component and suggests that alternative storage strategies or regular pruning will be necessary for practical deployment. The CPU utilization and memory usage increases are more moderate and should be manageable with modern hardware. The increased network bandwidth requirement (24.5 KB/auth) is also reasonable given the enhanced security features. The discrete event simulation provided comprehensive insights into the performance, security, and resource requirements of our proposed multi-factor authentication framework for OT environments. The framework demonstrates strong potential with high security scores and good resilience to network conditions but also reveals critical vulnerabilities that must be addressed before practical deployment. The comparative analysis confirms that our approach offers significant security advantages over traditional authentication methods, albeit with increased implementation complexity and resource requirements. With targeted improvements to address the identified vulnerabilities and optimize resource usage, the proposed framework could provide a robust security solution for critical infrastructure and OT environments.

In order to meet the strict 3 ms IEC 61850 latency constraint and ensure 99.999% availability for Zero-Trust MFA across 5G/TSN networks, a stateful cloud-edge structure with redundant verification nodes is necessary. Using credentials and policies pre-synchronized from a central cloud authority, this approach provides active/active pairs of lightweight Edge Verifiers (EVs) directly inside the factory's 5G/TSN fabric. This eliminates all WAN delay and jitter that lead to timeouts by enabling authentication decisions to be made locally at the edge in less than 1 ms. With a regional validator in the factory DMZ serving as a hot standby, high availability ensures uninterrupted operation even during connection disruptions and maintains the crucial sub-3 ms response time needed for GOOSE messages. If the regional EV fails, its peer takes over immediately.

Moreover, by installing a systems-based authentication proxy or gateway among the engineering terminals and the control network, a minimum viable MFA transition can be accomplished for PLCs and RTUs that are unable to be replaced. Before any OT protocol traffic can reach the endpoint, this gateway captures requests to connect to a legacy device (such as a request to program a PLC using its native protocol) and asks the user to authenticate. This approach satisfies IEC 62443 SL-2 criteria for authentication of users while not requiring any software modifications to the PLC/RTU itself by effectively front-dooring the existing device with an MFA checkpoint. By calculating the decrease in the risk of unwanted access, weighing the possible expense of a cyberattack regarding investment in the gateway hardware, software, and integration, and accounting for the avoided expense and disruption to operations of a complete hardware replacement cycle, the return on investment (ROI) of such a solution should be evaluated.

A quantifiable security–latency trade-off is introduced when Multi-Factor Authentication (MFA) is included into Operational Technology (OT) protocols like Modbus, DNP3, and OPC UA. This trade-off needs to be carefully handled to maintain system availability and real-time performance. MFA-related handshakes usually add 40–120 ms over session initiation for lightweight legacy protocols such as Modbus and DNP3, however if token caching or session persistence is utilized, the additional time each subsequent communication is less than 5 ms. On the other hand, OPC UA, which has native capability for secure authentication, only sees a 5–10% increase in CPU load and an 8–15% increase in negotiation latency, with no impact on throughput. In order to ensure that total latency stays within the 250–500 ms range usual for industrial operations, theoretical analysis establishes a threshold where verification latency ($T_a$uth) must remain below the residual of the system's control-loop deadline ($T_{(deadline)} - T_{(process)} - T_{(network)}$). According to empirical evidence, MFA preserves operational determinism and lowers the danger of unauthorized access

by up to two orders of magnitude when implemented at the current session or role-change level rather than per command. Because MFA strengthens security without sacrificing availability, it is therefore very useful in OT situations if it is developed with this security–latency balance in mind.

Alternative models could be developed from traditional perimeter defense toward Zero Trust Architecture, which is centered on Multi-Factor Authentication (MFA) as the key enforcement point for continuous verification. To ensure the robustness of the developed methods, formal methods such as TLA+ and Petri Nets could be applied to rigorously verify that the framework satisfies the safety invariants required by OT systems.

VIII. CONCLUSION AND FUTURE WORK

In conclusion, the integration of multi-factor authentication into an OT environment is one crucial step toward the furtherance of cybersecurity for critical infrastructures. Since cyber threats are becoming increasingly sophisticated in their nature, mere dependence on traditional security measures will no longer serve the purpose. MFA introduces a greater level of security by demanding multiple verification steps before access can be allowed, thus greatly reducing the chances of unauthorized access and breaches. Not only does MFA provide better security, but it also assists in bringing a sense of responsibility and alertness among organizations. By prioritizing cybersecurity in OT systems, organizations can protect sensitive data from attacks, maintain the integrity of operations, and assure the safety of essential services on which communities depend. Moreover, the adoption of MFA will proactively help solve the unique challenges that arise from the interconnection of systems and IoT as more industries move to adopt digital transformation strategies. Eventually, investment in robust cybersecurity measures like MFA is not only a technical but also a core responsibility that organizations need to assume to protect their assets and maintain public trust in the reliability and security of critical infrastructure.

The identified vulnerabilities in retina biometric (99.2%), blockchain (99.6%), and quantum channel (99.0%) components can be mitigated to below 5%, 2%, and 8% respectively through established techniques including liveness detection, Byzantine Fault Tolerant consensus, and decoy-state quantum protocols with post-quantum cryptography fallback.

In general, the industries are moving to complete digitalization. The future trends in cybersecurity for OT environments include some such as Increased Adoption of Zero Trust Architectures, MFA will play a critical role in enforcing Zero Trust principles by requiring continuous verification of user identities. Embracing the principles of "never trust, always verify" will empower organizations to navigate the complexities of modern cybersecurity challenges while maintaining operational efficiency and resilience. In addition, leveraging emerging technologies like AI, ML, and Quantum Computing to devise adaptive and context-aware authentication mechanisms to empower organizations to enhance their security posture with more operational efficiency by providing them with an integrated framework that combines these elements.

ACKNOWLEDGMENT

We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project.

CONFLICTS OF INTEREST STATEMENT

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

DISCLAIMER/PUBLISHER'S NOTE

The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

REFERENCES

[1] K. Stouffer et al., Guide to Operational Technology (Ot) Security, US Department of Commerce, National Institute of Standards and Technology, NIST, pp. 1–33, 2023. DOI: https://doi.org/10.6028/NIST.SP.800-82r3

[2] M. Nankya, R. Chataut, and R. Akl, "Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies," *Sensors*, vol. 23, pp. 1–31, 2023. DOI: https://doi.org/10.3390/s23218840.

[3] M. Marali, S. D. Sudarsan, and A. Gogioneni, "Cyber security threats in industrial control systems and protection," In Proceedings of the 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2019, pp. 1–7. DOI: https://doi.org/10.1109/ICACCE46606.2019.9079981.

[4] E. Perkins, "Operational Technology Security Focus on Securing Industrial Control and Automation Systems," 2014.

[5] A. Srivastava and A. Agarwal, "Emerging technology IoT and OT: Overview, security threats, attacks and countermeasures," *IJERT*, vol. 10, pp. 86–93, 2021

[6] A. Ometov et al., "Multi-factor authentication: A survey," *Cryptography*, vol. 2, pp. 1–25, 2018. DOI: https://doi.org/10.3390/cryptography2010001.

[7] N. F. Syed et al., "Zero Trust Architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3174679.

[8] C. C. Ike et al., "Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement," *Magna. Sci. Adv. Res. Rev.*, vol. 2, 074–086, 2021. https://doi.org/10.30574/msarr.2021.2.1.0032.

[9] V. Stafford, "Zero trust architecture," *NIST special publication*, 2020, 800, 800–207.

[10] S. L. Burton, "Advancing cybersecurity: Strategic insights into multifactor authentication," in Y. Chen (ed.), Organizational Readiness and Research: Security, Management, and Decision Making, Tempe, Arizona, USA: The Open Access Publisher (OAPL) 2025, pp. 247–282.

[11] J. Jose Diaz Rivera, A. Muhammad, and W. C. Song, "Securing digital identity in the zero trust architecture: A blockchain approach to privacy focused multi-factor authentication," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2792–2814, 2024. https://doi.org/10.1109/OJCOMS.2024.3391728.

[12] R. A. Grimes, Hacking multifactor authentication, John Wiley & Sons Inc., pp. 1–120, 2020.

[13] M. R. Alappat, "Multifactor authentication using zero trust," pp. 1–65, 2023.

[14] S. R. Kandula et al., "Context-aware multi-factor authentication in zero trust architecture: Enhancing security through adaptive authentication," *Int. J. Glob Innov. Sol. (IJGIS)*, vol. 1, pp. 1–77, 2024. DOI: https://doi.org/10.21428/e90189c8.f525ef41.

[15] J. Atetedaye, "Zero trust architecture in enterprise networks: Evaluating the implementation and effectiveness of zero trust security models in corporate environments," 2024.

[16] Y. Liu, "Analysis of Multi-factor Authentication (MFA) schemes in Zero Trust Architecture (ZTA): Current state, challenges, and future trends. *Int. J. Comput. Appl.*, vol. 186, pp. 30–36, 2024. DOI: https://doi.org/10.5120/ijca2024924310.

[17] D. Hanes et al., IoT fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, Cisco Press, pp. 110–244, 2017.

[18] M. Haugli-Sandvik, M. S. Lund, and F. B. Bjørneseth, "Maritime decision-makers and cyber security: Deck officers' perception of cyber risks towards IT and OT systems," *Int. J. Inf. Secur.*, vol. 23, pp. 1721–1739, 2024. DOI: https://doi.org/10.1007/s10207-023-00810-y.

[19] U.S. National Committee of the International Electrotechnical Commission. USNC Current, Vol. 19 No. 1–Winter 2024. https://share.ansi.org/Shared%20Documents/Standards%20Activities/International%20Standardization/IEC/USNC%20Current/News%20and%20Notes/Vol.%2019%20No.%201%20Winter%202024.pdf, 2024. Accessed: 2025-06-08.

[20] Y. Maleh, "IT/OT convergence and cyber security," *Comput. Fraud Secur.*, vol. 2021, pp. 13–16, 2021. DOI: https://doi.org/10.1016/S1361-3723(21)00129-9.

[21] Cisco Systems, "What Is OT Security?" https://www.cisco.com/site/us/en/learn/topics/security/what-is-ot-security.html, 2024. Accessed: 2025-06-08.

[22] M. Haugli-Sandvik, "Cyber risk perception in offshore operations: An exploratory study of deck officers' perceptions of cyber risks in norwegian shipping companies," 2024.

[23] N. Al-Alawi, "Evergreen ot security assurance: A sustainable approach to OT cybersecurity risk management," In *Proceedings of the SPE EOR Conference at Oil and Gas West Asia. SPE*, 2025, p. D021S018R007.

[24] M. Roopesh, "Cybersecurity solutions and practices: Firewalls, intrusion detection/prevention, encryption, multi-factor authentication," *Acad. J. Bus. Adm. Innov. Sustain.*, vol. 4, pp. 37–52, 2024.

[25] T. Suleski et al., "A review of multi-factor authentication in the internet of healthcare things," *Digit. Health*, vol. 9, p. 20552076231177144, 2023. DOI: https://doi.org/10.1177/20552076231177144.

[26] N. A. Sharma and M. Farik, "Security gaps in authentication factor credentials," *Int J Sci. Technol Res.*, vol. 5, pp. 116–120, 2016.

[27] O. M. Ogbanufe and C. Baham, "Using multi-factor authentication for online account security: Examining the influence of anticipated regret," *Inf. Syst. Front.*, vol. 25, pp. 897–916, 2023. DOI: https://doi.org/10.1007/s10796-022-10278-1.

[28] A. M. Mostafa et al., "Strengthening cloud security: An innovative multi-factor multi-layer authentication framework for cloud user authentication," Appl. Sci., vol. 13, 2023, pp. 30–75. DOI: https://doi.org/10.3390/app131910871.

[29] A. Akinsanya, "Securing the future: Implementing a zero-trust framework in us critical infrastructure cybersecurity. *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 10, pp. V1013–1221, 2024

[30] Siemens, "Multi-factor authentication for industrial use cases," https://blog.siemens.com/2023/02/multi-factor-authentication-for-industrial-use-cases/, 2023. Accessed: 2025-06-07.

[31] M. Noor et al., "Security and safety in cyber-physical system (CPS): An inclusive threat model," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 40, pp. 176–202, 2024.

[32] R. Shikhaliyev et al., "Cybersecurity risks management of industrial control systems: A review," *Probl. Inf. Technol.*, vol. 15, pp. 37–43, 2024.

[33] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber. Secur. Appl.*, vol. 2, p. 100031, 2024. DOI: https://doi.org/10.1016/j.csa.2023.100031.

[34] I. Ilanchezian et al., "Development and validation of an AI algorithm to generate realistic and meaningful counterfactuals for retinal imaging based on diffusion models," *PLOS Digital Health*, vol. 4, p. e0000853, 2025. DOI: https://doi.org/10.1371/journal.pdig.0000853.

[35] L. Semerád and M. Drahansky, "Retina recognition using crossings and bifurcations," in Applications of Pattern Recognition, IntechOpen, pp. 33–65, 2021. DOI: https://doi.org/10.5772/intechopen.96142.

[36] P. Pienimäki, "Vascular analysis from retinal images using machine learning methods," 2025.

[37] W. Ni et al., "Short-term exposure to ambient temperature variability and myocardial infarction hospital admissions: A nationwide case-crossover study in Sweden," *PLoS Med.*, vol. 22, p. e1004607, 2025. DOI: https://doi.org/10.1371/journal.pmed.1004607.

[38] J. Yoon et al., "Changes in optic nerve head microvasculature following disc hemorrhage absorption in glaucomatous eyes," *Sci. Rep.*, vol. 15, p. 3969, 2025. DOI: https://doi.org/10.1038/s41598-025-86460-7.

[39] A. Mahdi and F. Rabee, "DAGchains: An improved blockchain structure based on directed acyclic graph construction and distributed mining. *Mesopotam. J. Cybersecur.*, vol. 5, pp. 375–394, 2025. DOI: https://doi.org/0000-0002-9024-0731.

[40] F. Sabry,Blockchain Technology: Decentralized Systems Driving Innovation and Transparency in Modern Governance, One Billion Knowledgeable, 2025.

[41] S. M. Arafat, "A study of blockchain consensus protocols," *Cryptol. ePrint Arch.*, vol. 1, pp. 85–130, 2025.