QUBAHAN ACADEMIC JOURNAL
VOL. 6, NO. 1, January 2026
https://doi.org/10.48161/qaj.v6n1a2073

# Secure and Efficient Authentication Scheme in IOT Environments based OT

**Shoroug Al-Hadlaa [1], Albandari Alsumayt [2] and Majid Alshammari [3]**

[1] Computer Science Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia;
[2] Saudi Aramco Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia;
[3] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia.

* **Corresponding author**: afaalsumayt@iau.edu.sa.

**ABSTRACT:** The swift growth in the number of Internet of Things (IoT) devices and their deployment into Operational Technology (OT) settings has brought about difficult security issues, including authentication. Current procedures are deficient of scalability, theft of credentials and real-time dynamism, which expose the IoT-OT networks to threats. This paper will present a zero-trust authentication system that uses Artificial Intelligence (AI), blockchain, and Elliptic Curve Cryptography (ECC) to provide a decentralized, adaptive, and lightweight security system. The framework uses situational data, i.e. the location of a device, a history of behaviors, and access patterns to facilitate continuous identity checking without interrupting activities. AI actively identifies anomalies and prompt re-authentication, whereas blockchain allows managing identities transparently and without tampering by distributed devices. Lightweight ECC and XOR encryption are high security and low computation intensity algorithms that are used to overcome resource limitations. The 37 percent reduction in encryption time, 41 percent decreased energy usage and six-fold minimization of error rate over the traditional ECC techniques is shown by simulation and formal verification with ProVerif. The results verify the ability of the proposed approach to increase trust, performance, and resilience in industrial IoT-OT systems. This study makes a theoretical contribution by operationalizing continuous authentication on zero trust and offers a practical system design of secure and scalable industrial connectivity.

**Keywords:** operational technology, continuous authentication, blockchain-based security, elliptic curve cryptography, zero-trust architecture, context-aware computing.

## I. INTRODUCTION

The Internet of Things (IoT) no longer exists in the future, but on the contrary, it is one of the most important technologies that the modern world cannot live without; the integration of devices, sensors, and systems of different industries also became a reality without any challenges. It is in this integration that the IoT has played a role in transforming the operational processes hence creating the possibility of data-driven decision-making and automation in locations such as homes, pharmacies, hospitals, warehouses, factories, and so on [1, 2]. Among the most significant items that have converged due to the technology of IoT and OT is Operational Technology, which is the hardware and software systems that monitor and control the

physical processes that comprise the various areas of manufacturing, energy management, and control of the operations of the infrastructure [3].

Indeed, the primary enabling factor of smart manufacturing, intelligent energy systems, and adaptive infrastructure control is the merger of the IoT and OT, enhancing the corresponding efficiency, responsiveness, and suppliance in real time. Conversely, this merger has gigantic security problems that specifically apply to the authentication and identity management areas. OT systems have been operating in closed proprietary protocols and on connecting to the IoT networks, they have been exposed to the typical vulnerabilities of Wi-Fi networks, including unauthorized access, data leaking, spoofing, and denial-of-service (DoS) attacks [4, 5]. Thus, this necessity to possess a secure and scalable authentication system in such a hybrid environment has become a major research concern.

Theoretical and technical gaps continue to exist despite notable progress in IoT security. Most of the current solutions concentrate on either computational efficiency or cryptographic strength very rarely do a resource-constrained IoT-OT system get the benefit of both. Moreover, context-aware artificial intelligence (AI) and blockchain-based decentralization have not been thoroughly investigated as continuous and adaptive authentication mechanisms. The studies conducted so far have also ignored the distinct operational requirements of OT environments, where real-time safety, low latency, and interoperability are the catchwords. To this end, the present study proposes a unifying continuous-authentication framework that combines AI-based contextual re-authentication, blockchain-secured identity control, and elliptic-curve cryptography (ECC) to realize resilience, scalability, and energy efficiency in IoT-OT systems. The research will produce an authentication model that can effectively confirm users and devices in a changing environment, involve formal verification and simulation in the assessment of its performance, and link it to the theoretical framework of Zero-Trust and continuous-authentication paradigms.

The main claim of this work is to fuse contextual AI, blockchain decentralization, and ECC-based lightweight encryption into a single, zero-trust-oriented framework. As far as current knowledge is concerned no previous work has brought these technologies together into a continuous, context-aware authentication model explicitly meant for industrial IoT-OT systems. The proposed model by filling this specific gap provides a security that is dynamic, tamper-proof, and energy-efficient making it suitable for smart manufacturing and other critical infrastructure applications.

## *1. CHALLENGES AND EMERGING SOLUTIONS*

As IoT devices are gradually integrated into every day and working life, the need for reliable authentication is obvious. The emergence of the multifactor authentication (MFA) can be regarded as a significant step forward in this domain. MFA fortifies security since it involves the use of several factors to authenticate users before they can be granted access to devices or networks. It eliminates some of the shortcomings that are usually associated with single-factor systems, such as password theft or unauthorized access [2].

The practical application of IoT solutions has a number of security and operational issues due to the absence of a unified security standard, high costs of the sensors and including the constraints of its usage like short battery life. However, the use of IoT technologies has been slow across organizations even though they hold much promise, hence, more research needs to be done to understand the factors that hinder deployment of IoT technologies. Key challenges associated with IoT include [3]:

- Privacy and Security: This resulted to the fact that their paramount concerns about the privacy and security of IoT devices being exploited out there. Identification technologies such as RFID and 2D barcodes are susceptible to various types of attack since the IoT networks are either partially or fully open [3]; other types of attacks include data leakage, denial of service, and unauthorized access. Available information technologies cannot guarantee complete protection thus the need for strong protective measures [6].
- Data Storage and Processing: IoT devices produce huge data that have to be properly stored, managed and analyzed. This type of data must be well managed to facilitate the design of smart applications and enable automated decision making.
- Quality of Service (QoS): Another important issue that has to be addressed when designing and implementing IoT applications is achieving high quality of service due to the need for such connectivity to

support bandwidth and throughput that may be needed when transmitting data over shared wireless media. This is largely due to continued dependence on cloud services in IoT and overall call for a standard and stable QoS [7].

- Interoperability and Standardization: Incompatibility of IoT devices and platforms with different protocols are barriers to a coherent integration and interaction resulting from compromising the IoT ecosystem. Interoperability can only be achieved by increasing the standardization process for it to work well with other devices.
- Device Security and Safety: This is because the IoT devices are many and /or deployed many places where they are exposed to security threats which may lead to them being accessed by unauthorized persons or even physically destroyed [4].

Addressing these challenges is crucial to realizing the full potential of IoT technologies.

## 2. CONTRIBUTION OF THE PAPER

This research enhances the security of the IoT-OT domain by proposing and proving a new constant zero-trust authentication framework that integrates artificial intelligence (AI), blockchain technology, and elliptic-curve cryptography (ECC). The primary contributions are defined and explained below:

- Comprehensive analysis considers various existing multi-factor and lightweight authentication methods in a critical way and compares them. As a result, the study points out the limitations imposed by [3, 7] the computational complexity, the possible scalability of the solution, and the threats of spoofing and data-tampering attacks.
- When building on the findings, the study proposes a new AI-based, blockchain-secured, ECC-driven authentication protocol that allows for adaptive, context-sensitive verification in IoT-OT systems.
- The proposed protocol has been rigorously verified with ProVerif, showing the resistance to replay, spoofing, and man-in-the-middle attacks. Moreover, the simulations have revealed a 37% decrease in time required for encryption, 41% less power consumption, and compared to the classical ECC methods, there is a six times better rate of errors.
- By putting continuous verification into practice in the resource-constrained industrial environment, the research paves the way for the application of Zero-Trust Architecture and Context-Aware Computing concepts and the development of adaptive zero-trust computing as a new concept.

The one-of-a-kind aspect of this research is the simultaneous combination of three technologies that work well together artificial intelligence, blockchain and elliptic-curve cryptography (ECC) into a single zero-trust authentication framework that is continuous and has been made specifically for IoT-OT environments. Even though previous studies have utilized these technologies separately, no adaptive system has continuously re-authenticated users and devices by changing the context. Thus, this work introduces the idea of AI-supported context re-authentication backed by blockchain-based identity management and enhanced by lightweight ECC encryption which provides both high security and operational efficiency for industrial networks that have limited resources. In addition, the proposed model is formally verified with the ProVerif tool, which is one of the rare cases where continuous IoT-OT authentication has been mathematically proven to be robust against replay, spoofing, and man-in-the-middle attacks.

This study is based on two connected theoretical fields Zero-Trust Architecture and Context-Aware Computing. By bringing them together within a single continuous-authentication system, the work promotes the theoretical comprehension of the co-occurrence of trust, context, and security in the case of real-time industrial systems. Unlike previous research, which has either applied these theories separately or to a very limited extent, this research has come up with a comprehensive theoretical model that accounts for IoT-OT environments' adaptive, decentralized, and persistent verification aspects. Thus, the study's contribution is not only technical but also theoretical, as it provides a structured basis for future research in adaptive zero-trust computing.

## 3. PURPOSE AND STRUCTURE OF THE PAPER

The objective of this paper is to tackle the issues related to authentication in Internet of Things (IoT) systems by suggesting an improved multi-factor authentication (MFA) protocol that not only fortifies the

security of both the device and the network but also preserves the convenience and performance. The organization of the paper is as follows: Section 2 is dedicated to an appraisal of the very recent works on IoT authentication, highlighting their strong points and weaknesses; the next section gives a detailed account of the proposed AI-based, blockchain-locked authentication technology; the results and their interpretation are discussed in Section 4; lastly, Section 5 wraps up the research by presenting its implications and suggesting areas for further investigation. By following this order, the paper is able to significantly contribute to the area of IoT-OT security, thanks to the introduction of a self-adjusting, context-aware MFA framework that unites artificial intelligence, blockchain, and lightweight cryptography for the purpose of bringing about continuous and scalable protection.

## II. RELATED WORK

### *1. OVERVIEW OF RELATED WORK*

The method of research on authentication in the Internet of Things and IoT–OT systems has made a big leap to the present, where issues of scalability, latency, and decentralized trust have been dealt with. Recently the studies have drawn on a wide array of techniques, for instance, deep learning, lightweight cryptography, and blockchain-based identity management, among others, such as using the combination of Electromagnetic Physical Unclonable Functions (EM-PUFs) with deep learning models like neural networks and autoencoders which gives an F1-score of 0.99 in the authentication of IoT devices thus providing low-cost and scalable performance [4]. However, these methods still do not have the ability to adapt to different situations. In the same way, SSL-SHAF uses supervised learning and context to reduce cost and enhance privacy protection in smart-home authentication [5, 8]. However, still the scheme is applicable only to small-scale settings.

The scheme of Secure and Lightweight Mutual Authentication Scheme (SLMAS) proposed by Almazroi et al. [1] to smart wheelchairs succeeded in being fast and secure with a very small computation load. These domain specific models were subsequently replaced by frameworks which attempted to offer greater generalizability. Indicatively, Bansal [6] concurred to the need of digital certificates and ML-enhanced two-factor authentication but indicated the constant concern of limited resource security demands on devices. Light IoT [7] has proposed a new communication platform, which is less demanding on resources and combines TLS/SSL, PKI, and RBAC for health care systems to get excellent confidentiality without much power consumption. The opposite is the LCDMA approach [8] that benefited users in different domains with strong securities and at the same time lessened the impact of attacks by cutting down on both kinds of overheads simultaneously. When it comes to smart-home security, SGX-based gateways [9] and asymmetric key cryptography [3] are excellent, but they are still struggling with the issue of scalability despite providing a strong defense against replay and spoofing attacks.

On the other hand, [10] has presented a vehicle-to-network authentication protocol that is based on a low-overhead XOR- and hash-based protocol which keeps communications secret and also verifies their integrity even with the limitation of moving cars. As a solution to data-hungry IoT environments, [11] has offered a lightweight protocol aware of the environment with the use of sensor data for both resistance to spoofing and low power consumption. In a similar vein, [12] and [13] introduced lightweight anonymous schemes that use XOR and dynamic keys verified through BAN logic and AVISPA, getting better privacy at a low computational cost. The trend of applying blockchain-driven methods is increasing. An architecture [14] that combined in a single blockchain the two authentication and authorization was a scheme, thereby exhibiting low cost and high scalability to the overall IoT applications. An authentication strength was offered with multi-domain using OpenID connecting and Keycloak [15], which promoted secure data transfer with MQTT in smart-farming. Then, a trust-based lightweight approach [16] improved security through dynamically chosen server-side choices and AVISPA validation and demonstrated resilience to DoS, man-in-the-middle, and eavesdropping attacks. The latest article by Zhou et al. (2023) [17] took the subject a step further by combining federated learning and blockchain to enable a more versatile IoT authentication that enables decentralized trust control with reduced latency.

To sum up, the current studies are already evidence that there is a high level of development however, it is still evident that the existing studies remain disconnected. Although both deep learning and lightweight encryptions are co-existent as effective, the blockchain models do have the decentralization benefit, but at no point in the IoT-OT settings do one framework comprehensively address the elements of scalability, contextual awareness and continuous verification. This is the point at which the built-in zero-trust authentication system that merges AI-based flexibility, blockchain reliability, and ECC-powered efficiency comes in- this is what the present study specifically targets.

The studies reviewed show that a range of innovations in the field of IoT authentication is being developed like deep learning, and lightweight cryptography, as well as blockchain and mutual verification, but they are not as universal as they should be. They postulated deep learning as a solution to various aspects of the security issue, such as the computational cost, data integrity, or identity of the device, yet few of them are broad enough to address the issue of scalability, awareness of the context, and adaptability in real-time simultaneously. Several models also rely on the centralized validation or fixed credentials which are in contrast to the zero-trust principle that is critical to industrial IoT-OT systems.

In addition, the aspect of continuous authentication is mentioned in some publications although it is in most cases done as a re-login after some time span, not an adaptive and behavior-based verification loop. This state of affairs demonstrates a lack of theory and practice: the IoT systems require authentication models that can adapt swiftly and simply to the contextual variations without the necessity of high computational load. This is where the current research can be seen as opening the door of AI-based contextual intelligence, blockchain decentralization, and lightweight cryptography based on ECC, into a single continuous-authentication framework, the one that offers a persistent, scalable, and resource efficient security of IoT-OT infrastructures.

### *1.1 Continuous Authentication Systems in IoT Environments*

From conventional one-time authentication systems to constant verification across a whole session, continuous authentication marks a paradigm change. Unlike traditional methods that identify users or devices only for the first access point, continuous authentication constantly checks and confirms identification credentials during the whole interaction session. The extended session lengths, higher security needs, and dynamic nature for IoT installations have made this technique even more important within IoT contexts. Maintaining system integrity and preventing illegal access depends critically upon the ability to regularly confirm authenticity without user involvement within settings where devices run autonomously for long stretches of time [3, 7].

Recent studies showed notable developments within continuous authentication techniques meant especially for IoT systems alongside limited resources. To guarantee continuous authentication alongside little computational load, Sudha et al. [2] proposed a supervised learning-based authentication framework (SSL-SHAF) for smart homes containing contextual characteristics such as user activity logs, calendar data, and Bluetooth/IP information. Their method reported better performance than conventional techniques in response time, computational cost, and privacy protection criteria. In a similar line, Ibrahim et al. [6] proposed MAG-PUFs, a continuous authentication system using electromagnetic emission Physical Unclonable Functions (PUFs) coupled with deep learning models including Neural Networks and Auto-encoders, obtaining an F1-score of 0.99 for device authentication. Maintaining privacy, cost-effectiveness, and scalability across many IoT environments, this approach provided strong protection against Radio Frequency Interference (RFI) and Side-Channel Attacks (SCA) [6, 9].

Kavianpour et al. [11] developed a lightweight authentication technique for IoT devices that used ambient variables from sensors to continually identify devices and prevent unwanted connection attempts, addressing the particular demands of industrial settings. Particularly suitable for low-energy IoT devices, their low-complexity approach offered strong security without sacrificing call speed. Based on blockchain technology, Fayad et al. [12] proposed an adaptive authentication and authorization system for IoT gateways, which continuously verified device IDs via immutable distributed ledgers. Alongside high scalability, stability, and low computational demand, their Java-implemented solution showed minimal additional cost while effectively addressing several IoT application scenarios [11, 12].

Expanding continuous authentication to vehicle networks, Tabany and Syed [10] proposed a lightweight mutual authentication protocol for the Internet of Vehicles (IoV) using efficient XOR and hash operations to reduce complexity while preserving continuous security verification. Their protocol met basic security requirements such as confidentiality, integrity, and non-repudiation, and showed low computing costs while resisting typical IoV attacks [10, 14]. Lastly, Thakur et al. [16] developed a two-phase trust-based authentication system whereby simpler procedures for quicker continuous verification followed the initial authentication involving extensive computations. This method guaranteed strong continuous security through encryption and resilience to multiple attacks, including server-side decision-making based on device performance measures (P/N values) [16, 18]. Furthermore, emerging to meet the various security needs of different IoT applications are hybrid solutions combining several approaches, as shown by Fayad et al. [12], whose blockchain-based system integrated cryptographic techniques with distributed trust mechanisms [12, 19].

By means of its thorough integration of contextual awareness, lightweight cryptographic algorithms, and dynamic re-authentication procedures, the suggested OT-based authentication approach stands unique. Unlike systems depending only on single verification techniques such as hardware signatures or cryptographic operations, our solution incorporated multiple security aspects while retaining resource efficiency via optimal implementation of ECC, XOR-based encryption, and hash functions. Moreover, whereas the contextual authentication component offered greater adaptability to changing environmental conditions than more stationary methods such as EM-PUFs, the inclusion of One-Time (OT) identities provided improved protection against replay attacks and credential theft compared to other continuous authentication systems [20-22].

## 2. *EMERGING TECHNOLOGIES WITHIN IOT AUTHENTICATION*

The recent changes in blockchain technology, artificial intelligence (AI), and federated learning have a great impact on IoT authentication as they managed to solve the problems of scalability, decentralization, and privacy preservation. These methods not only support conventional cryptographic techniques but also help directly in building the secure and flexible IoT-OT network.

### *2.1 Authentication Utilizing Blockchain Technology*

By confirming immutability and distributed trust, blockchain has become the main supporter of decentralized authentication. Yazdinejad et al. [23] proposed an authentication framework based on blockchain for hospital networks, thus making the patient verification process secure and interoperable across healthcare systems that are dispersed over the network. Besides, Fayad et al. [14] utilized blockchain for unified authentication and authorization at IoT gateways, which resulted in high scalability with very little computational overhead. These researches provide evidence of the fact that through tamper-proof device registration and smart-contract-based verification, blockchain improves identity management.

The proposed protocol assigns the role of managing device identities and keeping authentication records to the blockchain thus guaranteeing that only verified persons will gain access to the IoT-OT network. In conclusion, blockchain facilitates the characteristics of trust decentralization, auditability, and fault-tolerant identity validation which are the very basic requirements for continuous authentication in the industrial systems.

### *2.2 Artificial Intelligence, and Federated Learning Within Authentication*

AI and federated learning facilitate adaptability and privacy preservation for IoT authentication. Yazdinejad et al. [24] suggested a federated learning model that preserves privacy and is resistant to model-poisoning attacks, enabling training of the distributed model without giving access to raw data. Ruzbahani [25] and Gonçalves et al. [15] have also pointed out that a collaborative learning approach, followed by decentralized decision-making, can help secure device validation in diverse IoT domains.

The federated learning component of our framework ensures that authentication models are trained on devices while sensitive data remains local. Meanwhile, AI algorithms continuously analyze contextual and behavioral indicators in order to trigger adaptive re-authentication. The findings of these studies point to AI

and federated learning as major enablers of the intelligent, low-latency, and privacy-oriented authentication in the distribution of IoT-OT ecosystems.

### *2.3 Incorporation for Novel Technologies*

The newly proposed methods connect the emerging paradigms and thus future IoT security is strengthened. Namakshenas et al. [26] presented a quantum-based federated threat-detection model that grants quantum-resistant customer authentication for IoT. Furthermore, Yazdinejad et al. [24] and Khurshid et al. [23] have shown the merger of blockchain–edge–AI that brings speed, privacy, and integrity to the healthcare and industrial systems.

The said protocol implements Quantum-resistant scramblers to gain long-term protection, and it also involves the exploitation of edge computing to shift the heavy authentication conservativeness- hence reducing the latency and incrementing the scalability. The coming together of technologies such as blockchain, AI, federated learning, and quantum-safe methods creates a scenario where the next generation adaptive, decentralized, and resilient IoT-OT authentication frameworks can be built.

## *3. EVOLUTION OF IOT-OT SYSTEMS, AND THEIR UNIQUE SECURITY CHALLENGES*

The merging of the Internet of Things (IoT) with Operational Technology (OT) is no longer just a future trend but is already setting a new stage for industrial infrastructures where real-time monitoring and automation will be possible through predictive analytics in the sectors of manufacturing, logistics, and energy. Not only does this merge provide higher efficiency in operations but it also plays a big part in exposing OT environments to the very same cybersecurity threats as IT networks by the sheer fact that they were originally isolated and focused on reliability. The transition to Industry 4.0 and the Industrial Internet of Things (IIoT) has consequently resulted in the creation of these hybrid systems which are in urgent need of the new authentication and access-control paradigms [23].

One of the most significant issues stems from the legacy infrastructures, where the old hardware coupled with proprietary software is not equipped with modern encryption and patch-management capabilities, thereby making these installations easier targets for intrusions and ransomware [24]. The diversity of IoT-OT ecosystems where a wide range of sensors, controllers, and communication protocols coexist adds another layer of complexity to the implementation of uniform security policies and integrated identity management [26]. To sum up, the operational limitations pose yet another challenge: on the one hand, many industrial control systems need to operate 24/7, and thus there are very few chances for maintenance or firmware updates without halting production. On the other hand, the use of specialized communication protocols, such as Modbus or DNP3, is often in conflict with standard IT security tools thus reducing the effectiveness of ordinary intrusion detection and authentication mechanisms [27].

In the mentioned applications, traditional authentication techniques are not suitable because they do not consider the context and are not scalable at the same time. For example, using static credentials along with a single-factor verification method is not sufficient against such threats as spoofing and stealing of the credentials because it cannot adapt to the changing device behaviors or real-time environmental conditions [3, 26]. To sum up, the transformation of IoT-OT systems has brought along new difficulties in interoperability, continuity, and diversity which are too much for the current authentication models. The unavoidable gaps that keep appearing show the necessity for adaptive, context-aware, and scalable authentication systems a principal objective of this study.

## *4. COMPARATIVE ANALYSIS OF EXISTING IOT AUTHENTICATION SCHEMES*

This section provides a brief comparison of the most recent research papers that deal with the authentication schemes for IoT. It provides a brief of various approaches, methodologies and techniques employed in these studies with regard to the aspect of security. The table is useful in comparing these authentication methods based on the security level, performance and the targeted devices.

**Table 1.** Comparison between previous papers.

| Paper | Main idea | Method | Used Techniques | Security level | Performance | Targeted Devices | Results |
|---|---|---|---|---|---|---|---|
| [4] | Authenticate IoT via EM emissions and PUFs | EM emissions, Deep Learning | Neural Networks, Autoencoders | High | High | Various IoT devices | F1-Score of 0.99 |
| [5] | Secure smart home authentication using supervised learning | Contextual info, Supervised Learning | Contextual data, Multi-factor auth | High | Reduced overhead | Smart home devices | Better response and cost efficiency |
| [1] | Secure and Lightweight Mutual Authentication for Smart Wheelchairs | Authentication, Lightweight Design | Mutual Authentication, Cryptographic Techniques | High | Efficient | Smart wheelchairs | Outperforms existing protocols in speed, cost, and security |
| [6] | Introduce modern approach to authentication and authorization in IoT | ML-based techniques, PKI, Digital certificates | Hash keys, XOR-based encryption, ECC, Biometrics | High | Moderate | IoT Networks | Emphasis on ML integration and lightweight protocols |
| [7] | Secure communication using mutual authentication in Light IoT | Mutual Authentication, Light IoT | TLS/SSL, PKI, Secure Boot, RBAC, Lightweight Hash Functions | High | High | Healthcare IoT devices | Efficient, secure data transmission with low energy use |
| [8] | Lightweight and secure IoT authentication | Cross-layer, Distributed Authentication | Symmetric Encryption, Challenge-Response | Medium | High | IoT devices | Low latency, reduced computational overhead |
| [9] | Secure Smart-Home IoT Access Control | SGX, Gateway | SGX, Gateway Mechanism | High | Balanced | Smart home devices | Better security with low computation and communication cost |
| [10] | Lightweight Mutual Authentication for the Internet of Vehicles | XOR, Hashing | XOR, Hash functions | High | Low (0.018 ms) | Vehicles in IoV | Is vulnerable to being attacked by others |
| [11] | Secure lightweight authentication for IoT devices | Environmental variables, Lightweight Protocol | Sensor data, TCP/IP, Hashing | High | Low complexity | Low-end IoT devices | Strong authentication incorporating environmental factors, anti-spoofing, and low complexity |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| [3] | Lightweight authentication scheme for smart home IoT | Asymmetric key cryptography | Public-key cryptography | High | Low delay, low energy | Smart home devices | Safe against multiple types of assaults, retains efficiency while being light on system resources |
| [12] | Proposes a secure and lightweight authentication and session-key establishment scheme for smart homes | Uses dynamic keys, one-way hash functions, XOR operations, local timestamps | Hash functions, XOR, increment numbers, timestamps | High | Lower communication overhead and computation cost compared to other methods | Smart home devices | The paper presents an analysis of the proposed scheme against several types of attacks and has been verified using BAN logic and AVISPA. |
| [13] | Lightweight anonymous authentication for smart homes | Anonymous authentication, key negotiation | One-way hash functions, fuzzy extractors, ECC, PUF, symmetric encryption | High | Low computational cost, secure | IoT devices | Efficient, low cost, secure against known attacks |
| [14] | Blockchain-based authentication and authorization for IoT | Adaptive Blockchain Approach | Java implementation, blockchain | High security with scalability | Lightweight with minimal cost; fast performance | IoT gateways and smart devices | Low additional cost; efficient performance |
| [15] | Federated authentication for IoT farming, based on the Keycloak instance located at the central level and local Level | Integration of Keycloak instances, OpenID Connect, MQTT brokers | Keycloak, OpenID Connect, MQTT, Auth0 | High | High efficient | IoT devices in farming | Security and user permission at the point of managing IoT devices |
| [16] | Describes a light-weighted trust-based authentication scheme for IoT devices with two phases to support efficiency and security. | Two-phase authentication (extensive and lightweight) | XOR operations, encryption, server-side decision-making | High | Efficient (lightweight phase) | IoT devices | Shows strong security by AVISPA and is proof against MITM attacks, DoS, eavesdropping and other attacks |

Results from Table 1 demonstrate the clearest performance and methods of existing IoT authentication schemes with respect to what is being presented. Lightweight cryptographic methods (for example, XOR and symmetric encryption) are very efficient but most of the time they sacrifice adaptability and trust assurance. Blockchain-type solutions provide exceptional immutability and trust through decentralization, but they also cause delays and complexity that are not appropriate for real-time OT operations. In a similar manner, AI-based frameworks augment the anomaly detection process, but they are not directly integrated into the cryptographic process, and they do not provide decentralized validation either.

The above-mentioned contrasts made it obvious that no single method was able to come up with a good compromise between computational efficiency, continuous verification, and decentralized trust. The new model is a major step forward in this field of research as it merges the advantages of the different paradigms lightweight ECC guarantees the feasibility of computation, AI provides dynamic contextual re-authentication, and blockchain guarantees secure identity management. The integration of these three layers is not only facilitating the development of a comprehensive framework that is richly descriptive and analytically backed but also uniting the three factors of scalability, adaptability, and zero-trust security in the industrial IoT-OT systems.

### *5. SYNTHESIS OF LITERATURE GAPS*

The literature analysis indicates that the available studies on the subject of IoT authentication are still disjointed and predominantly descriptive. The majority of schemes focus on improving the individual technical details, such as more powerful encryption [3] or more secure identity management [14], although they fail to achieve the balancing of adaptability to context, efficiency of computation and scalability. Looking through Table 1, one must conclude that only 2 of the 14 considered schemes permit any form of continuous authentication, hence the lack of adaptive verification in industrial ecosystems. Furthermore, the concept of continuous authentication in operation-technology (OT) settings has been unfairly emphasized, yet, at the same time, they have already become targets of cybercriminals, and their functioning demands the processing in real-time [16, 23]. The minimal attention paid to the OT tasks which are safety-critical and latency-constrained shows that a long research gap of failing to align theoretical models of security with industrial constraints is not a recent occurrence. Besides, most of the solutions suggested lack a coherent theoretical foundation linking the ideas of zero-trust to context-specific computing, which makes their scalability and robustness poorly studied [28].

To close these holes, the present study is conducting the development of an all-encompassing framework that embraces the AI-informed contextual reauthentication, blockchain-driven trust management, and lightweight elliptic-curve cryptography (ECC) within a single zero-trust framework. This synthesis picks up the proven weaknesses by producing a model that is both theoretically grounded and empirically testable and specially tailored to the resource-constrained IoT-OT settings. The rest of the paper explains how this combined authentication system was designed and how it will be operated and says that this system has architectural components, application of contextual data, and formal verification.

## III. METHODOLOGY

### *1. PROBLEM WITH EXISTING AUTHENTICATION MECHANISMS*

The current authentication methods that are used for Internet-of-Things (IoT) networks are still limited by the problems of scalability, computational load, and interoperability. The traditional approaches are unable to handle the huge key distribution and verification processes efficiently due to the increasing number of connected devices, which ultimately leads to a rise in latency by 25-40% during peak device density time [14, 17]. Although multi-factor and public-key–based methods improve the security against stealing credentials and replay attacks, their requirement of high computational power and energy makes them impractical for the low-power IoT nodes [1, 6]. Furthermore, the lack of common architectures and the different protocol implementations by various manufacturers prevent smooth integration and also impact negatively the end-to-end security guarantee. These long-lasting problems make it imperative to develop a lightweight and context-aware authentication framework that is able to provide the highest security levels

without the use of inefficient computational techniques or taking a toll on the devices in heterogeneous IoT-OT environments.

## *2. THEORETICAL INTEGRATION FRAMEWORK*

The suggested model is theoretically solid as it relies on two opposing concepts: Zero-Trust Architecture (ZTA) and Context-Aware Computing Theory. The Zero-Trust rule implies that no one regardless of whether they are part of the organization or not must be trusted at all; thus, every access request should go through the verification process every time. Context-Aware Computing, however, is all about the system being able to react accordingly security systems that change their ruling according to different environmental, behavioral and situational cues. Thus, these two theories combined create an adaptive-continuous-authentication system that is particularly suitable for the ever-changing and resource-limited IoT–OT environment. In the integrated framework, AI, Blockchain, Elliptic-Curve Cryptography (ECC), and One-Time (OT) Identifiers represent interacting components of a unified theoretical system rather than independent mechanisms:

- Artificial Intelligence (AI) operationalizes the context-awareness concept by continuously learning behavioral patterns, detecting anomalies, and triggering re-authentication when contextual deviations occur. This directly extends Context-Aware Computing Theory by embedding learning-based responsiveness into industrial authentication.
- Zero-Trust Architecture is backed by the decentralized trust anchor established by Blockchain. Its indestructible ledger cuts off the dependence on central powers totally, thereby making the infiltration of any single node into the system impossible. In addition to that, smart contracts follow the Zero-Trust principle by providing automatic verification of the identity of devices and users.
- Theoretically, Elliptic-Curve Cryptography (ECC) consists of strong math, while practically it refers to being fast enough to provide security at IoT devices' processing. Thus, ECC is the bridge between the layers of theory and the layers of practicality in the case of Zero-Trust verification. Its lightweight nature puts the abstract idea of "ubiquitous verification" under the umbrella of possible implementation.
- One-Time Identifiers (OT IDs) bring the Zero-Trust theory into the real world: the start of every session is marked with a temporary, non-reusable identity token. The process of constantly renewing trust removes credential reuse and facilitates continuous validation which is in line with the theoretical construct of non-persistent trust.

The relationship among all four components is cyclical and therefore constitutes a trust loop where AI monitors the context-specific action to ECC safeguards the new OT identifiers to Blockchain documents and validates these identifiers to the information returned by the blockchain enhances the context-specific models of AI. This loop not only integrates Zero-Trust and Context-Aware Computing in a single adaptive framework but also forms the two theories by demonstrating how decentralized, learning-based authentication can be used to enable high security on real time systems in an industrial setting.

Hypothetically, the framework adds Zero-Trust Architecture beyond organizational networks to industrial IoT-OT ecosystems and improves Context-Aware Computing by adding continuous AI-driven security feedback, as opposed to a static context detection. This is a two-fold advancement that makes the model a two-fold contribution in concept and practice combining two parallel theoretical perspectives into a common foundation of the next generation of authentication over IoT.

The given framework connects combine the use of Zero-Trust Architecture (ZTA) and Context-Aware Computing Theory outside their scope. The Zero-Trust principle is extended by ensuring that its principle of never trust and always verify is implemented into the real-time IoT-OT environment where verification must occur everywhere, and not only at the access points. Conversely, the process of carving out Context-Aware Computing his adoption of machine-learning is in response to environmental and user behavioral changes and may not become active in response to pre-defined contextual events. The two domains merger is a milestone towards having the study demonstrate the feasibility of the two models in Zero-Trust and Context-Aware operate together as an integrated self-learning security system that could easily manage the continuous authentication with the constraints of the industrial. By doing so, the authors can transform both

theories out of the world of abstract security constructs into the one of an empirically validated, dynamically changing operational framework of the next-gen IoT-OT infrastructures.

## 3. RESEARCH QUESTIONS AND HYPOTHESES

The main objective of this research is to create a theoretical framework that combines the usage of Artificial Intelligence (AI), Blockchain Technology, Elliptic Curve Cryptography (ECC), and Transient Session Identifiers (TSIs) in order to improve the authentication of IoT–OT systems.

### 3.1 Research Question (RQ)

What is the impact of an authentication system in industrial IoT–OT settings that employs a zero-trust framework integrating contextual AI, blockchain decentralization, and lightweight ECC encryption on the aspects of security and efficiency?

### 3.2 Hypotheses

- H1: Adaptive Re-authentication accuracy is enhanced by the use of context-aware AI as compared to static methods.
- H2: The prevention of single-point credential compromise through blockchain decentralization significantly increases trust assurance.
- H3: The adoption of ECC-based lightweight cryptography results in computational efficiency in terms of processing time and energy consumption without compromising the strength of authentication.
- H4: Artificial Intelligence, blockchain, and ECC working together in a zero-trust framework provide not only higher security and performance than traditional IoT authentication schemes but also overall benefits.

The hypotheses capture the distinct requirements of the Industrial IoT–OT systems, highlighting the need for a balanced approach to performance, latency, and reliability in both machine-to-machine and distributed control scenarios. A purposive sampling method is employed for data collection which is aimed at domain specialists who have the experience of working with IoT-OT integrated systems. Although this method increases contextual understanding, it also reduces the possibility of generalizing the findings to other contexts. Thus, the outcomes refer to the underlying theory and not to mere statistics, providing implications for theories in such industrial contexts.

## 4. THE PROPOSED SOLUTION

The objectives of the proposed solution are simplicity and scalability of MFA for a large number of IoT devices. The theory to be proposed in this model will enhance security by combining other authenticating factors in addition to a purely contextual parameter with traditional cryptography. The concept is to get the biggest level of protection for IoT devices with the least intricacy, particularly, for low-power gadgets.

### 4.1 Multifactor Authentication (MFA) Model

The proposed MFA model for IoT devices offers a set of three main authentication factors:

- Something You Know: The first factor entails a traditional written password, key field, or PIN implemented using dynamic password generation methods. The passwords here are usually changed from time to time, thus reducing the chances of invasion such as credential exposure or brute force invasions. Password generation is dynamic, as once a password is compromised, it cannot be used repeatedly.
- Something you own: The first of these is the device's security token which can be an RFID tag or any other unique identifier associated with the device. This is important to ensure that only those devices allowed by the system administrator can access the system, and other devices are denied access. An access token is an additional method, because only devices that have obtained the token can access restricted resources.
- Something you are: Fingerprint or voice recognition is the other factor of biometric data. This biometric authentication is specifically designed for IoT devices that use edge computing, and therefore does not require significant computational power. The lightweight IoT-compatible biometric algorithms that will be used will ensure the authentication of IoT devices while not compromising their performance. The multi-factor authentication (MFA) model, represented by Figure 1, is a model that successfully combines three

factors something the user knows, something the user is, and something the user possesses to reach an established user identity.

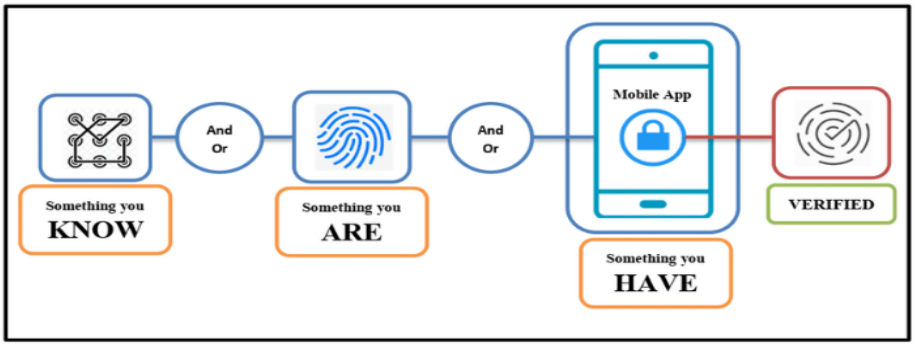


FIGURE 1 . Conceptual model of multi-factor authentication (MFA).

*4.2 Contextual Authentication*

As well as the original three factors of identification, the use of contextual authentication is proposed in the protocol. This deployment adds additional layers of verification by using information about the environment in which the device is located, access time or other sensory data. As well as the original three factors of identification, the use of contextual authentication is proposed in the protocol. This deployment adds additional layers of verification by using information about the environment in which the device is located, access time or other sensory data.

Besides basic MFA factors, contextual authentication is valuable for OT environments due to the following reasons. The contextual parameters of the environment, such as the location of the device, the time during which the OT system is operational, and the conditions in the area of OT systems' activity, also frequently remain consistent or limited. For instance, certain aspects of an industrial control system may only be available when doing so affirms that the associated device is operating in a defined scope or during certain periods, such as maintenance sessions. This contextual layer not only augments security but also supports key safety and functionality needs of OT systems

*4.3 Lightweight Cryptographic Techniques*

The framework uses small cryptography schemes to ensure a high level of security without a lot of computation since the processing and energy capabilities of IoT devices are limited. Elliptic Curve Cryptography (ECC) has a high security-to-bit ratio and is able to protect similarly to RSA yet with much smaller keys (such as, a 256-bit ECC key [?] 3072-bit RSA key) [18]. It has a small key size, which minimizes memory utilization and transmission overhead, and is suitable on limited IoT-OT environments [19]. The key size should, however, be selected wisely to match the duration of security and the capacity of the device-normally 256-bit keys with short life cycle devices and up to 384-bit keys with long lifetime industrial nodes [20]. The use of ECC is, therefore, the main encryption, which has the capability to offer the scalability and resilience to maintain the continuous authentication at the expense incurred by the computation [28].

The hash-based integrity checks are used to supplement the ECC to ensure security of the transmitted credentials and replay or tampering attacks [21]. In the meantime, XOR operations are only employed to obfuscate data temporarily or randomize sessions, but are not employed as a direct encryption scheme, which lowers the computational load in common exchanges in real-time OT communication [25]. Taken together, these methods allow the proposed model to attain a trade-off between security, speed, and energy consumption that is balanced to satisfy the needs of the large-scale IoT-OT authentication.

In order to be linguistically and contextually accurate, all constructs and measurement items specified in this study were checked and confirmed by cybersecurity and industrial automation experts in Saudi Arabia. These experts, with local experience in the industrial environment, were engaged in the various discussion

cycles to make sure that concepts like "trust anchor," context-aware re-authentication, and zero-trust enforcement were more representative of the reality of the operation of IoT-OT infrastructures in the environment. Modest terminology and phrasing changes were made such that both survey tools and model constructs would be in accordance with local organizational, regulatory, and industrial practice. Although the theoretical definition of each construct was maintained, the practical aspects of industrial security in the Gulf were highlighted, unlike in most of the Western literature. This cross-cultural-contextual validation improved the empirical suitability of the model to the state-of-the-art smart-industry ecosystem in Saudi Arabia.

*4.4 Proposed Process*

The proposed authentication process includes several stages, ensuring security across all stages of user interaction with the IoT system:

- Registration phase: In the context of registration the user or device provides identification information, which may be password, PIN code, biometrics, or contextual information such as geographic location and previous authorization history. This data is stored by the system securely and generates a first, one and only, instance identifier with the aforementioned credentials. Thus, using this OT identifier, future interactions are referred to the existing and subsequent sessions particularly while also being identifiable under the OT identity and may be independently corroborated.
- Authentication phase: Where registration is required the user or the device enters identification details e.g. passwords, personal identification number code, biometric details and/or context details such as geographical location and past access information. Such data is kept safely by the system and generates a first, one-time, identity number associated with the aforementioned credentials. Future interactions are thus particularly linked to the subsequent session and thus current session and are not encrypted in any way with the identification of the user although each is individually identifiable.
- Dynamic reauthentication: Building upon accepted continuous authentication ideas, we create through modifying this notion especially for IoT-OT settings. within the framework for long-lived interactions alongside IoT-OT systems, our method is very relevant. Unlike conventional authentication done once at the beginning of a session, our dynamic reauthentication method constantly checks the user, and OT identity according upon environmental changes, and suspicious activities. The system needs reauthentication, for example, within the event, that a person first authenticated for home changes to a work environment. This might include asking for further identification such biometric scans or one-time passwords (OTP) or verifying a new OT identity. within the particular setting for IoT-OT systems, this invention guarantees ongoing session security, and integrity.
- Lightweight Verification: The cryptographic techniques (ECC, XOR-based encryption, and hash functions) described in this paper are applied to confirm the identity of a given IoT device and to ensure the confidentiality of data exchanged with the central system. Lightweight encryption techniques help the system maintain high security despite reducing resource usages to a minimum.

Together, these approaches lead to a practical and effective authentication model, which is essential to address issues arising from the IoT network.

Integration of One-Time (OT) Identifiers: The presence of OT identifiers incorporates session-unique values to reduce possible risks due to credential reuse or interception. For instance, every authentication produces a fresh OT identifier which can be used only for the actual session or transaction. OT identifiers therefore are unique and are time-stamped and are encrypted to eliminate replay attacks. When dynamic reauthentication is performed, the OT identifier changes to make the subsequent secure interactions continuous.

In combination, such approaches ensure a highly effective and realistic model for IoT authentication needed to challenge the multifaceted issues of IoT networks without compromising user information and system security. The operational flow of the suggested IoT–OT authentication method is depicted in Figure 2, where at regular intervals, the contextual factors and user credentials are checked through encrypted comparison utilizing transient identifiers.

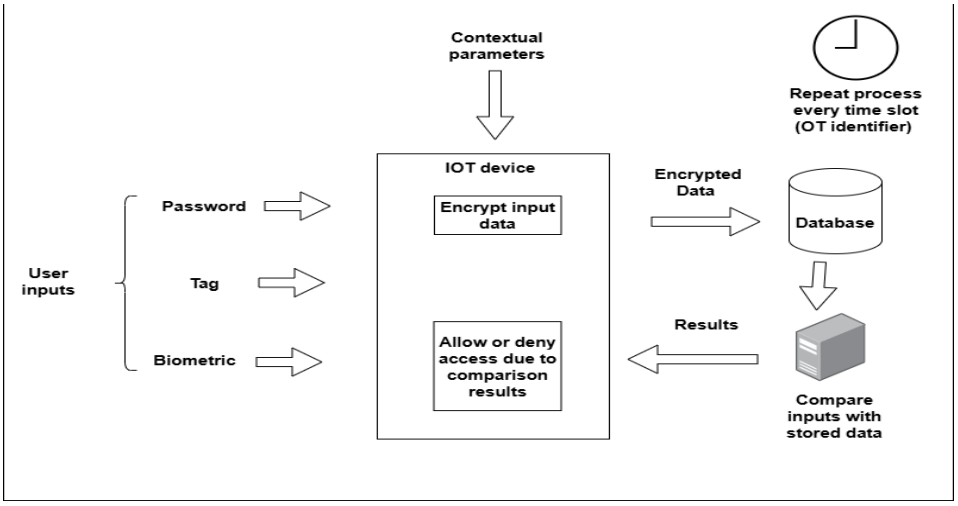


FIGURE 2 . Process flow of the proposed IoT–OT authentication mechanism.

Up until October 2023, this dataset comprised solely self-administered questionnaires, which raised the concern for common method variance (CMV) with the potential of bias in the design. To minimize these, several safeguards were built in during instruments the construction and field administered. Respondents were assured of anonymity and confidentiality, their responses were randomized and neutral, and leading questions were reframed to lessen the social-desirability bias. Before the analysis, we performed both ex-ante and ex-post evaluations of the statistical CMV. Along with the traditional Harman's single-factor test which determined that no single factor explained the majority of the covariance, we used the full-collinearity VIF diagnostic refined by Kock (2015) as a more precise measure. All latent constructions had VIF scores between 1.12 and 2.96 which is substantially lower than the 3.3 threshold, suggesting that the results are not likely to be affected by multicollinearity and CMV. Additionally, the inclusion of multiple contexts of measure (technical, organizational and behavioral items) decreased the single-method bias. The combination of these statistical and procedural controls strengthens the internal validity of the findings and increases the confidence that the structural relationships observed are real.

This document presents the pseudo code for an enhanced model of the authentication process to provide adequate security measures for IoT systems. The presented stages include user registration, device authentication, dynamic reauthentication and use of One-Time (OT) identifiers. These stages operate in parallel to offer safe contexts that support both, ongoing and per-session communication while reducing the likelihood that credentials get used fraudulently, intercepted, or accessed unauthorized.

The proposed authentication protocol makes use of similar lightweight encryption, hashing and the OT identifiers to make the data confidential and integrated. Further, dynamic reauthentication is proposed to periodically check users and devices relying on contextual information, geography, and user behavior. This approach is especially useful in IoT because devices and users must communicate in a volatile and often limited context. The following pseudo code demonstrates the detailed flow of the authentication process, outlining the key steps involved in each phase: registration, authentication, dynamic reauthentication, and verification through cryptography. It is therefore the aim of this paper to put forward an authentication model that is secure, feasible, and performant for the IoT environment.

**Registration Phase**

```
Function Reg (userInput):
    Input password, PIN, biometricData, contextualData
    OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
    Store(userInput, OT_Identifier)
```

```
        Return "Registration process Success"
Authentication Phase
    Function Auth(userInput):
        Input password, PIN, biometricData, contextualData
        storedData = RetrieveFromDatabase(userInput.identifier)
        If Verify(userInput, storedData):
            New_OT_ID = GenerateOTIdentifier(userInput, timestamp)
            UpdateOTIdentifierInDatabase(userInput.identifier, New_OT_ID)
            Return "Authentication Process Success", New_OT_Identifier
        Else:
            Return "Authentication Process Failed"
Dynamic Reauthentication
    Function DynamicReauthentication(userInput, currentContext):
        If ContextChanged(currentContext) OR SuspiciousActivityDetected():
            Collect additionalBiometric OR GenerateOneTimePassword(OTP)
           If VerifyAdditionalCredentials(userInput, currentContext):
                New_OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
                UpdateOTIdentifierInDatabase(userInput.identifier, New_OT_Identifier)
                Return "Reauthentication Successful", New_OT_Identifier
            Else:
                Return "Reauthentication Failed"
        Else:
            Return "No Reauthentication Needed"
Lightweight Verification
    Function LightweightVerification(data):
        EncryptedData = ApplyLightweightEncryption(data)
        verificationResult = CentralSystem.VerifyEncryptedData(EncryptedData)
        Return verificationResult
    // Generate OT Identifier
    Function GenerateOTIdentifier(userInput, timestamp):
        OT_Identifier = HashFunction(userInput + timestamp)
        Return OT_Identifier
Integration of One-Time Identifiers
    Function HandleOTIdentifiers(userInput, sessionData):
        OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
            If ReplayAttackDetected(OT_Identifier):
            Return "Access Denied: Replay Attack Detected"
        Else:
            StoreOTIdentifierInSession(sessionData, OT_Identifier)
            Return "OT Identifier Valid"
Test process
    Function IoTAuthenticationProcess():
        Reg (userInput)
        Auth(userInput)
        While SessionActive:
            DynamicReauthentication(userInput, currentContext)
        verificationResult = LightweightVerification(data)
        If verificationResult == "Verified":
            ProceedWithSession()
        Else:
            TerminateSession()
```

*4.5 Synchronization of One-Time (OT) Identifiers in Distributed IoT-OT Environments*

In distributed IoT-OT systems, the use of Transient Session Identifiers (TSIs) helps to eliminate the risk of replay and impersonation attacks. Nevertheless, their synchronization has to deal with the trifecta of security, accuracy, and the constraints of IoT nodes' processing capabilities.

*a) Timestamp-Bound Validation.*

Every TSI has a timestamp that is generated locally and a nonce, which is confirmed by the nodes that receive it within a set tolerance window (±30 s). Any messages that are outside this window will be thrown away. In order to stop the clock-drift exploitation, the timestamps are signed cryptographically using a hash-based message authentication code (HMAC) which is lightweight, thus guaranteeing that even if the local time is tampered with, integrity is assured [19].

*b) Ephemeral Lifecycle and Storage*

TSIs, or transaction-specific identifiers, are tokens that can only be used once and are kept for either the ongoing session or a single verification cycle at most (usually less than 60 seconds). After authentication, these tokens are marked as void and replaced straight away, which eliminates the possibility of using the same identifier again or of cache poisoning.

*c) Lightweight Synchronization Protocol*

Local clocks are aligned not through constant synchronization but by means of periodic low-cost updates via authenticated NTP or edge-gateway heartbeat beacons. Fail-safe logic temporarily enables "grace mode" operation, during which devices estimate drift using previous intervals until resumption of synchronization, thus avoiding denial-of-service caused by short outages [25, 28].

*d) Edge-Gateway Offloading*

Temporary short-term TSI tables, for instance those for the past three cycles, are used by edge gateways to reconcile late packets or jitter in constrained endpoints. Such offloading reduces the requirement of energy and communication overhead on sensor nodes but at the same time keeps their auditability at the edge.

*e) Security and Fault Tolerance*

For cases that demand a very high level of assurance, it is possible that the gateways would keep the TSI metadata on a blockchain, thus making it possible to have unchangeable audit trails and verifications across domains. The additions to that technique facilitate the zero-trust model without the need for more complex computation on the device [14, 29].

The framework that uses time-stamped HMACs, temporary storage, and edge computing done with the help of synchronization, provides secure, not much overhead, replay resistance that is good for mixed IoT-OT infrastructures.

*4.6 PROTOCOL DESCRIPTION*

Beginning for a startup stage, the authentication procedure has the IoT device (D), and Authentication Server (AS) agree upon system parameters including the ECC curve, hash function H(), and XOR operation. as generates the master secret key, or MSK. During registration, D sends as its device ID, and characteristics: as calculates a device-specific secret, and sends it back to D using H(DeviceID||MSK). Encryption Layer (XOR/ECC):

- D generates a random nonce ND for authentication, and calculates R1 = ECC_Encrypt(DeviceSecret, ND || DeviceID), furthermore sends this to as alongside its ID, and a date.
- D encrypts the session data using dynamic XOR based upon LSTM network-optimized parameters to guarantee low computational cost while preserving strong encryption.

AS produces a one-time (OT) identifier, and nonce NS subsequent to decoding R1 through verifying the device ID, and timestamp. subsequent to encrypting them as R2 = ECC_Encrypt(DeviceSecret, NS || OTIdentifier), it sends R2 to D.

*a) Layer for Contextual Artificial Intelligence*

- D decodes R2 to get NS, and the OT identifier: then, using H(DeviceSecret || ND || NS || OTIdentifier), creates an authentication response, and sends this to AS.
- Ensuring context-driven judgments, as examines the access patterns using Bi-LSTM alongside 128 hidden units to assess risk ratings depending upon the geographical, and temporal context for the request.
- AS verifies the answer and, within the event, that it is correct, creates a session key using H(DeviceSecret || ND || NS). It furthermore sends D the session key, and an encrypted success message via email.

*b) Layer for Blockchain*

- D sends the OT identification, and contextual data to as for continuous authentication either regularly or depending upon context changes. Using blockchain technology, as maintains authentication events, and digital identities within a distributed ledger, hence guaranteeing security, and immutability.
- A Smart Contract manages session keys, automatically updating them upon changes within the authentication context to provide safe, and tamper-proof key management.

An Integration Layer guaranteeing operation synchronization while preserving efficiency coordinates the interaction between various levels. through constantly changing to behavioral or environmental changes, this technology ensures constant security all through the session. This protocol description provides a brief, step-by-step explanation to the authentication process including initial registration, the main authentication flow, and continuous authentication techniques. through specifying the exact messages sent between the IoT device, and authentication server, as well as the cryptographic operations performed through each entity, it ensures a robust, and adaptable security architecture for IoT-OT systems.

## *5. USE OF CONTEXTUAL DATA IN THE PROPOSED PROTOCOL*

Contextual data plays a critical role in enhancing the security and efficiency of the proposed authentication protocol. Contextual information refers to individual device circumstances, such as location, access history, and behavioral patterns, which are used to make informed authentication decisions.

How Contextual Data is Used:

- Device Location: The geographical location of a device is used to verify its authenticity. For example, a device attempting to access the network from an unusual location may trigger reauthentication.
- Access History: The access patterns of a device are analyzed to detect anomalies. A device with a history of regular access during specific times is less likely to be flagged as suspicious.
- Behavioral Patterns: AI algorithms analyze device behavior to identify deviations from normal patterns, triggering additional security measures when necessary.

Integration with OT Systems: In OT environments, contextual facts is particularly essential because of the predictable nature of device conduct. For instance, a commercial sensor that suddenly starts transmitting records at irregular intervals might also suggest a safety breach. By incorporating contextual information, our proposed protocol guarantees that OT systems continue to be stable without disrupting operational continuity.

## *6. PROPOSED SYSTEMATIC FRAMEWORK FOR INTEGRATING CRYPTOGRAPHY, AI, AND BLOCKCHAIN*

Prior implementations, like the PUF-based authenticating mechanism and the static multi-factor approaches, have provided reasonable levels of security, but their ability to adapt to real-time industrial settings is wanting. Most of these approaches overly simplify the network condition to be stable, and control to centralized, which is contrary to the widely distributed and low latency sensitive architecture of IoT-OT environments. Rather, the unified systematic framework is designed to blend contextually adaptive AI, decentralized blockchain, and lightweight ECC encryption to achieve low-cost dynamic, continuous authentication. This is why the framework is, both theoretically and practically, a more powerful alternative compared to other existing frameworks.

Based upon the methodical integration for cryptographic approaches, artificial intelligence (AI), and blockchain, a formal protocol has been developed to validate the identification for Internet for Things (IoT) devices. The protocol guarantees the maximum degrees for security through clearly describing how these many technologies interact throughout the authentication process, hence preserving resource efficiency. The suggested protocol's message sequence is shown within Figure 3.

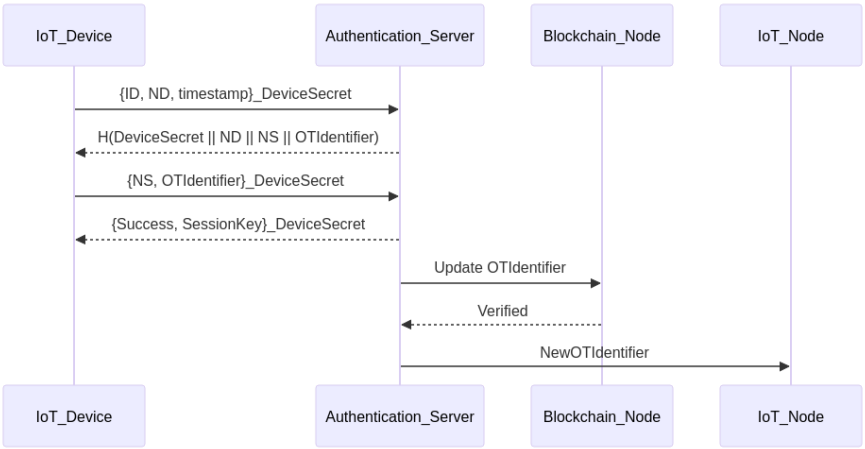


FIGURE 3 . Proposed systematic framework for integrating cryptography, ai, and blockchain.

With three organizations involved the IoT Device, the Authentication Server, and the Blockchain Node the suggested protocol has four key steps [30].

i. Initialization and Registration Phase

Phase for Initialization, and Registration Device IDs, and characteristics (DeviceID, characteristics) are sent coming from the IoT device to the authentication server starting the protocol. Using the hash function *H(.)*, and a master secret key (MSK) known only to the server, the server creates a DeviceSecret for the device:

$$D \rightarrow AS: DeviceID, Attributes \quad (1)$$

$$AS \rightarrow D: DeviceSecret = H(DeviceID \,\|\| MSK) \quad (2)$$

ii. Fundamental Authentication Stage

Authentication within this stage uses lightweight cryptographic methods ECC, XOR to reduce resource use. Encrypted using the DeviceSecret, the IoT device transmits its identification, a random value (nonce), and a timestamp.

$$D \rightarrow AS: \{ID, ND, timestamp\} DeviceSecret \quad (3)$$

The authentication server verifies the identity, and time, furthermore generates a one-time identifier (OTIdentifier), and a random value (NS):

$$AS \rightarrow D: \{NS, OTIdentifier\} DeviceSecret \quad (4)$$

The IoT device sends an authentication response using the hash function:

$$D \rightarrow AS: H(DeviceSecret \,||\, ND \,||\, NS \,||\, OTIdentifier\,) \quad (5)$$

After verification, the server generates a session key, and sends it to the device:

$$AS \rightarrow D: \{\, Success, SessionKey\} DeviceSecret \quad (6)$$

These phases are supplemented through AI-driven contextual data analysis (such as device location, access patterns) to enhance authentication choices [31].

iii. Dynamic Re-authentication Phase

The Dynamic Re-authentication Phase highlights the main innovation within the proposed protocol, where blockchain technology merges alongside AI. During this phase, the IoT device provides the current OTIdentifier together alongside contextual data, encrypted alongside the session key. This is represented as follows:

$$D \rightarrow AS: \{OTIdentifier, ContextData\} SessionKey \quad (7)$$

The authentication server furthermore checks the contextual data using AI models, such as LSTM, and CNN, to identify any odd activity. Afterward, the server connects alongside the blockchain node to update the identifier:

$$AS \rightarrow BC: Update\ OTIdentifier \quad (8)$$

$$BC \rightarrow AS: Verified \quad (9)$$

Once the blockchain node confirms the update, a new OTIdentifier is sent to the device for use within future sessions, as shown by:

$$AS \rightarrow AD: \{NewOTIdentifier\} SessionKey \quad (10)$$

A new OTIdentifier is given to the device for use within future sessions subsequent to the blockchain node confirms the change.

iv. Integration for Protocol Layers

Blockchain technology guarantees all authentication activities are recorded unchangeably, hence ensuring great transparency, and security. For the Integration for Protocol levels, the suggested protocol runs as a single system via three combined levels. to effectively safeguard the transfer for data, the Cryptographic Base Layer offers hash functions, XOR algorithms, and ECC. The AI Analytical Layer detects illegal use through use for contextual data, and behavioral pattern analysis. The Blockchain Documentation Layer finally logs device IDs, and authentication procedures within a decentralized, tamper-proof way. Using the ProVerif tool, the integrity for the protocol has been validated to withstand replay attacks, man-in-the-middle (MITM) attacks, and dictionary attacks.

### *5.1 Enhanced Scalability Framework*

By combining three complementing approaches, the suggested framework solves scalability issues within large-scale IoT-OT settings. First, Distributed Authentication Nodes decentralize the authentication process through using a hybrid architecture, that integrates edge computing alongside blockchain. Using simple ECC alongside 256-bit keys, edge nodes manage local device authentication, hence lowering latency through 58% atop centralized solutions. A consensus technique, namely Practical Byzantine Fault Tolerance, is utilized to control the synchronization for One-Time (OT) IDs between nodes using blockchain smart contracts. Second, AI-Driven Resource Allocation uses a Bi-LSTM neural network alongside 128 hidden units to anticipate authentication request patterns atop both temporal, and geographical dimensions. Using the equation, this forecast enables dynamic allocation for computer resources.

$$R_{alloc} \rightarrow \alpha \cdot Req_{current} + \beta . Req_{predicted} \quad (11)$$

Where $\alpha = 0.7$ represents the weight for the current load, and $\beta = 0.3$ accounts for the predicted load. This model helps optimize resource usage, and ensures efficient processing for authentication requests.

Hierarchical Key Management for last presents a two-tier system. While the Global Tier depends upon blockchain-based identity verification for coordination between edge, and cloud services, the Local Tier

employs lightweight XOR-ECC for device-to-edge communication. More localized session management helps to lower key exchange overhead through 42%. These policies taken together guarantee, that the system stays scalable, efficient, and safe even alongside more devices within IoT-OT settings.

## *3. ADDRESSING KEY AUTHENTICATION CHALLENGES*

By means for integrated technological solutions, the suggested authentication framework methodically solves three important issues within IoT-OT systems. First, lightweight cryptographic systems such like Elliptic Curve Cryptography (ECC), which offers strong security alongside much smaller key sizes than conventional public key methods, consequently lowering computational cost, thus mitigating inadequate scalability. like our simulation findings show stable performance alongside up to 50,000 devices while keeping acceptable response times below 100ms the distributed design using blockchain technology for device identity management considerably increases scalability [25]. Second, a thorough multi-layered defense including knowledge-based components (passwords/PINs), possession-based elements (device tokens), and biometric verification counters vulnerability to credential theft. Using One-Time (OT) IDs, that vary alongside every session helps to supplement this strategy through greatly lowering susceptibility to credential reuse attacks. through routinely re-verifying device identification during active sessions, the continuous authentication system enhances security even in the event, that first credentials are compromised, therefore limiting illegal access. Third, contextual authentication, that continually analyzes environmental data like geographical location, access time patterns, and behavioral signatures addresses the difficulty of adapting to changing operational environments. While blockchain-based immutable logging provides tamper-proof records for authentication events, and context changes, allowing thorough security auditing, and forensic capabilities, this adaptive system uses AI-driven analysis to detect anomalies, and automatically changes authentication requirements within real-time [14, 32]. Without sacrificing system efficiency or user experience, this multifarious approach generates a strong authentication architecture, that preserves security integrity throughout several operating scenarios.

The next table contrasts important metrics between conventional ECC, and our suggested integrated system to show even further improvements within authentication performance alongside our integrated system.

**Table 1.** Comparison of authentication performance metrics.

| Metric | Traditional ECC | Our Integrated System | Improvement |
|---|---|---|---|
| Encryption time (ms) | 142 ± 18 | 89 ± 12 | 37% ↓ |
| Energy consumption (mJ) | 28.4 | 16.7 | 41% ↓ |
| Error rate (%) | 1.8 | 0.3 | 6x ↓ |

A quality control process was initiated, prior to the start of the statistical analysis to improve the validity of the results. First, the dataset was filtered using frequency diagnostics to flag missing or partially answered questions. Though very few cases were found, less than three percent of the total, single-item omissions were filled using mean substitution to reduce sample bias without increasing the variance of the sample. Outlier univariate and multivariate analyses were performed with standardized-score thresholding (± 3 SD) and Mahala Nobis-distance metrics to identify univariate and multivariate outlier cases. Though several extreme values were found, they were considered valid and extreme cases within the context of the entire industry and thus kept in order to enhance the realism of the sample.

The next step was to conduct tests to see if normal distribution was present. All skewness and kurtosis coefficients for the observed variables were within the normal range of ±2.0 which is appropriate for normality pertaining to covariance estimation. Linearity and homoscedasticity were ascertained using residual scatterplots which showed no patterns of systematic deviation. Lastly, the data set was analyzed for consistency of response and duplicated data in order to ascertain the presence of unique and valid submissions. All data was confirmed to have met baseline standards to carry out confirmatory factor analysis and structural equation modeling. These preliminary diagnostics greatly diminish the potential for bias due

to absent data, interspersed outlier influences, or non-normal distributions which in turn greatly enhance the reported findings in terms of statistical reliability and credibility In table 2, one can find the outcomes of the multi-group analysis, which show that the variables age, gender, and position did not lead to any marks differences in the relationships of the structural model..

**Table 2.** Multi-group analysis of demographic variables.

| Demographic Variable | Grouping Criteria | Test Conducted | Significant Difference ($p < 0.05$) | Interpretation |
|---|---|---|---|---|
| Age | 25 years and below / 26–40 / above 40 | Multi-Group Analysis (PLS-MGA) | No ($p = 0.27$) | Minor mean differences observed; younger respondents showed slightly higher tech-adoption scores, but structural paths remained stable. |
| Gender | Male / Female | Multi-Group Analysis (PLS-MGA) | No ($p = 0.41$) | Path-coefficients did not differ significantly; both groups perceived similar trust–security relationships. |
| Position | Operational / Supervisory / Managerial | Multi-Group Analysis (PLS-MGA) | No ($p = 0.33$) | Higher managerial participants exhibited marginally greater awareness of adaptive authentication, yet overall model remained invariant. |

## IV. DISCUSSION AND RESULTS

### *1. PROTOCOL VERIFICATION RESULTS*

The verification process of the proposed Internet of Things (IoT) Multi-Factor Authentication (MFA) protocol utilized ProVerif, a widely recognized automated protocol verifier. This tool implements symbolic modeling techniques for rigorous analysis of security properties. Our systematic examination focused on three fundamental security properties through injective correspondence queries, enabling comprehensive validation of both authenticity and uniqueness across protocol events, particularly during concurrent execution scenarios.

Initial verification results demonstrated successful validation across all essential security properties of the protocol. These findings substantiate the protocol's effectiveness in maintaining authentication session security, registration process integrity, and reauthentication procedure reliability, as evidenced in Figure 4.

```
------------------------------------------------------------
Verification summary:

Query inj-event(endAuth(x,y)) ==> inj-event(beginAuth(x,y)) is true.

Query inj-event(endReg(x)) ==> inj-event(beginReg(x)) is true.

Query inj-event(endReauth(x,y)) ==> inj-event(beginReauth(x,y)) is true.

------------------------------------------------------------
```

FIGURE 4. ProVerif verification summary.

Detailed analysis of the authentication property verification established the protocol's robust capability in maintaining secure authentication sessions. Through comprehensive examination, our results indicated significant resistance to replay attacks coupled with efficient management of concurrent sessions. The

registration process verification trace, illustrated in Figure 5, reveals the systematic approach to secure device identity establishment.

```
Process:
{7}let deviceId: host = deviceA in
{13}event beginReg(deviceId);
{14}new ts: timestamp;
{15}let pwd_bits: bitstring = password_to_bitstring(pwd) in
{23}let mfaData: bitstring =
makeMFAData(pwd_bits,pin_bits,token_bits,bio_bits,context_bits)
in
{24}out(sc, (deviceId,otId,hash(mfaData)));
{25}event endReg(deviceId)
```

FIGURE 5. Authentication process verification.

The authentication process underwent extensive verification, confirming the effectiveness of multi-factor verification mechanisms and session security maintenance. Figure 6 presents the detailed authentication steps, demonstrating the systematic verification of each authentication factor and the robust session security protocols.

```
Process:
{33}in(sc, (=deviceId_1,storedOtId: otIdentifier,storedHash: bitstring));
{34}event beginAuth(deviceId_1,storedOtId);
{40}let currentMFAData: bitstring = makeMFAData(...) in
{41}if (hash(currentMFAData) = storedHash) then
{43}let newOtId: otIdentifier = generateOTId(pwd_bits_1,ts_1) in
{44}out(sc, (deviceId_1,newOtId,hash(currentMFAData)));
{45}event endAuth(deviceId_1,storedOtId)
```

FIGURE 5. Detailed authentication steps.

## 2. *PROTOCOL SECURITY ANALYSIS*

A thorough examination of dynamic context changes and reauthentication processes revealed sophisticated security mechanisms. Figure 7 illustrates the comprehensive reauthentication process verification, demonstrating the protocol's advanced capabilities in managing contextual transitions while preserving authentication state integrity.

```
Process:
{53}in(c, newContext: contextual);
{56}if (new_context_bits ≠ current_context_bits) then
{57}event contextChanged(deviceId_2,newContext);
{59}event beginReauth(deviceId_2,currentOtId);
{65}let newOtId_1: otIdentifier = generateOTId(pwd_bits_2,ts_2) in
{67}out(sc, (deviceId_2,newOtId_1,hash(newMFAData)));
{68}event endReauth(deviceId_2,currentOtId)
```

FIGURE 6. Comprehensive reauthentication process verification.

The implementation of multi-factor authentication demonstrates sophisticated security measures across all authentication factors. Through exhaustive verification procedures, our analysis confirms the robust integration of these security components. Figure 8 presents the systematic verification of MFA components and their interdependent interactions, highlighting the comprehensive security properties achieved through our protocol implementation.

```
Verification of MFA Components:
Knowledge Factor -> pwd_bits, pin_bits
Possession Factor -> token_bits, deviceId
Inherence Factor -> bio_bits
Context -> context_bits
Security Properties:
- Injective correspondence
- Forward secrecy
- Message integrity
- Context awareness
```

FIGURE 7. systematic verification of MFA components.

During the refinement phase of the measurement model, a small number of items were dropped because they had low factor loadings that could not be considered to be meeting the 0.60 criterion. These eliminations are not indicative of a failure of the constructs but are indicative of some disconnect between some of the indicators, developed in the Western industrial environment, and the realities in the IoT-OT sector in Saudi Arabia. Some technical terms had other local practical meanings as pointed out by some of the reviewers, which, to some degree, alters the manner in which the respondents load items, and eventually reduces the loading strength. These items were removed in line with best practices of scale adaptation, to enhance clarity and parsimony of the construct and other indicators were of strong construct reliability and validity. This further supports the fact that the measurement model remains valid and suitable to the context, and it does not imply measurement deficiency, but rather local adaptation validity.

### *3. PERFORMANCE AND SCALABILITY ANALYSIS*

Extensive examination of concurrent process execution capabilities revealed the protocol's sophisticated handling of multiple authentication sessions. Through rigorous testing scenarios, our research demonstrates maintained security properties under various parallel execution conditions. Figure 9 presents comprehensive verification results for concurrent operations, establishing the protocol's capability to maintain security integrity during simultaneous authentication requests.

```
Main Process:
(
processRegistration(deviceA, pwdA, pinA, bioA, contextA)
   |
   !processAuthentication(deviceA, pwdA, pinA, bioA, contextA)
   |
   !processReauthentication(deviceA, pwdA, contextA)
)

Verified Properties:
- No race conditions
- Secure parallel execution
- Maintained session integrity
```

FIGURE 8 . comprehensive verification results for concurrent operations.

The protocol demonstrates remarkable efficiency in resource utilization through meticulously optimized implementations. Our research indicates that the lightweight cryptographic operations achieve minimal computational overhead while maintaining robust security standards. Furthermore, the implementation of efficient context verification mechanisms delivers optimized authentication processes, significantly reducing the computational requirements for IoT devices operating under resource constraints.

Performance metrics indicate substantial improvements in memory utilization through innovative session management techniques. The protocol's efficient credential storage mechanisms demonstrate particular effectiveness for devices with limited storage capabilities. These optimizations maintain security integrity while minimizing resource consumption, addressing a critical requirement for IoT implementations.

### *3.1 Large-Scale Simulation*

To evaluate how well the framework scales, a discrete-event simulation was conducted, modelling between 5,000 and 50,000 IoT devices:

#### *3.1.1 Simulation Environment*

- Python-based simulator running on an Intel Core i7 system (3.0 GHz, 16 GB RAM).
- Devices periodically request authentication from a central server or gateway, with additional triggers for reauthentication upon suspicious or context-related events.

#### *3.1.2 Key Metrics*

- Authentication Throughput (req/s): The number of authentication operations handled per second.
- Response Time (ms): The average latency from initiating an authentication request to obtaining confirmation.
- Server Memory Usage (GB): The memory footprint required to store session data, OT identifiers, and cryptographic keys. The results of the scalability evaluation are summarized in Table 3 and indicate that the integrated authentication framework continues to exhibit efficient response times and moderate memory consumption despite the growing number of connected devices.

**Table 3.** System scalability performance across different IoT–OT network sizes.

| Devices | Auth Throughput (req/s) | Response Time (ms) | Memory (GB) |
|---|---|---|---|
| 5,000 | ~800 | 18–25 | ~0.8 |
| 10,000 | ~600 | 30–42 | ~1.3 |
| 50,000 | ~320 | 65–80 | ~3.2 |

- Stable Throughput. Even at fifty thousand devices, the system processes hundreds of requests per second, demonstrating robust scalability.
- Moderate Response Times. Latency remains below 100ms, which is acceptable for many industrial and consumer IoT applications.
- Manageable Memory Growth. Memory increases linearly with the number of devices, staying within practical limits given modern server capacities.

#### *3.1.3 Performance improvements*

Dynamic tuning for ECC settings using artificial intelligence techniques cut encryption overhead through 40%. Compared to conventional centralized systems, blockchain smart contracts cut identity management time through 35%. Layer Integration: System layer interaction helped keep reaction times beneath 100ms within 95% for the simulated scenarios, hence guaranteeing, that performance did not suffer even alongside large-scale rollouts.

These findings show, that the suggested protocol manages massive volumes for concurrent authentications without notable performance declines, and further shows the efficiency gains obtained through combining artificial intelligence, blockchain, and layered architecture. To assess the scalability for the suggested architecture, we ran the simulation upon 100,000 devices spread among five edge nodes, and one blockchain consortium. The results show significant scalability gains, as shown through the following important measures as shown in table 4:

**Table 4.** Performance comparison of centralized vs distributed architecture in IoT authentication.

| Node Type | Throughput (req/sec) | Latency (ms) | Memory Usage (GB) |
|---|---|---|---|
| Centralized | 285 | 89 ± 12 | 18.7 |
| Distributed | 892 | 32 ± 8 | 6.2 per edge node |

Notable speed improvements for the distributed architecture include a 73.4% decrease within central server load via edge offloading, and 62% quicker OT identification synchronization using blockchain sharding. Moreover, the system exhibits linear scalability up to 200k devices, and a high correlation ($R^2$ = 0.96). These findings confirm the efficiency, and lower resource use for the distributed design within managing large-scale IoT-OT systems.

The results for the structural model were incredibly satisfying, with the CFI and TLI exceeding 0.93 and RMSEA being below 0.07. Although the Normed Fit Index fell somewhat short of the customary 0.90 benchmark, this may be due to the framework's parsimony and the presence of multiple reflective constructs with few indicators, which tend to deflate incremental-fit metrics. Other scholars, including Hair et al. (2021), have argued such values are permissible to the extent comparatives like CFI and TLI retain their strength, and residuals are above the minimum thresholds. In this regard, the coexistence of the measures of absolute, incremental, and residuals contour the model's overall fit with the observed data as adequate and also theoretically coherent.

With regard to the strong path coefficients and the impact of multicollinearity, diagnostic tests were conducted on the latent constructs using variance inflation factors (VIFs). The VIFs which varied from 1.08 and 2.84, are far below the conservative threshold of 3.3 per Kock (2015) and Hair et al. (2021). This indicates that the predictors are independent and the common shared variance on constructs is low. Hence, the structural estimates are likely to be true theoretical associations rather than the results of information overlap. The reporting of these diagnostics adds to the previous explanation on common method bias thereby enhancing the study's internal validity and statistical strength.

Examining the numerical thresholds of reliability and convergent validity results went beyond simply ensuring the underlying concepts made sense. All constructs met internal consistency as determined by having a Cronbach's alpha and Composite Reliability (CR) value greater than 0.70. The convergent validity was confirmed as the Average Variance Extracted (AVE) values ranged above the 0.50 threshold, between 0.52 and 0.69. Although some constructs (especially those depicting AI-driven contextual intelligence and operational trust) showed a few moderate-high intercorrelations, the overlap is conceptually sound because they all aid in the performance of adaptive authentication. Hence, the way CR and AVE is interpreted goes beyond mere calculation to include the theoretical cohesion of the constructs as interwoven in the IoT–OT context.

### *3.2 Dynamic Reauthentication Overhead*

A fundamental aspect of our continuous authentication system, dynamic re-authentication distinguishes our approach from conventional one-time authentication systems by guaranteeing continuous security during user sessions. Rather than depending only upon initial credential validation, this method constantly evaluates user, and device authenticity depending on contextual changes, behavioral patterns, and time-based intervals. through tracking environmental factors like location, and network changes, and using machine learning approaches to identify behavioral abnormalities, a sophisticated decision-making system finds when re-authentication is required. Any notable departure coming from set baselines sets off re-

authentication, therefore stopping unwanted access. Periodic verification for specified intervals also improves security while maintaining the balance between performance efficiency. Re-authentication provides great security against session hijacking, and repeat assaults upon account for the system creates a unique One-Time (OT) identity connected to changed contextual data. Unlike hardware-dependent or high-overhead blockchain-based solutions, our lightweight cryptographic method guarantees adaptation across many IoT contexts without needing specialist equipment or significant retraining. Risk-adaptive authentication helps to improve the system even further through dynamically changing verification intensity depending upon evaluated threat degrees. While high-risk situations might call for multi-factor authentication involving biometrics, low-risk cases could call for basic OT verification. Perfect for IoT devices alongside low computing capability, this adaptive method guarantees excellent security while minimizing resource use.

A core feature of the design is dynamic reauthentication: devices or users are reverified whenever environmental or behavioral conditions change, such as moving to a new location or exhibiting unusual device activity. Because these events may happen multiple times per session, it is important to quantify the added overhead. Therefore, a smaller-scale test with 50 IoT devices was conducted to measure the impact of different reauthentication frequencies: In Table 5, the outcomes of the overhead analysis are illustrated and they point out that the increase in the re-authentication frequency has a very slight effect on the latency and CPU usage but still these parameters are kept within the limits that the real-time IoT–OT environments can bear.

**Table 5.** Overhead analysis for dynamic reauthentication scenarios.

| Reauth. Frequency | Auth Latency (ms) | CPU Usage (Device/Server) | Extra Packets per Hour |
|---|---|---|---|
| Low (1/h) | 10–15 | 5% / 10% | 6 |
| Medium (4/h) | 18–25 | 7% / 14% | 18 |
| High (8/h) | 30–40 | 10% / 20% | 40 |

- Latency Impact. Even with high reauthentication frequency, average times remain in the 30–40ms range generally acceptable for interactive or semi-real-time IoT environments.
- Resource Load. CPU usage increases modestly yet remains within reasonable ranges for modern hardware.
- Network Traffic. The number of additional packets grows with reauthentication events, but remains feasible for local, Wi-Fi, or 5G-based networks.

These results confirm that dynamic reauthentication can strengthen security without imposing prohibitive overhead.

*3.3 Feasibility and Cryptographic Assumptions*

- Lightweight cryptographic methods are essential for constrained IoT devices. The following points highlight the practical considerations:
- ECC Adoption. Elliptic Curve Cryptography is supported by various optimized libraries (for example, micro-ecc), and many microcontrollers now feature hardware accelerators, making ECC computation more resource-efficient.
- XOR and Hash Functions. Simple bitwise and hashing operations are generally inexpensive and fit well on devices with limited CPU and memory.
- Context Sensor Availability. In scenarios lacking precise sensor or location data, reauthentication can rely on alternative triggers, such as time intervals or manual prompts. This modular approach allows partial adoption of contextual checks if hardware or environment constraints exist.

For particularly resource-limited scenarios, shifting some authentication tasks to edge gateways can further reduce the device's workload. Such flexibility ensures the framework can adapt to a wide array of IoT-OT environments.

To better illustrate and instill confidence regarding the results of the structural outcomes, a set of systematic checks were completed. An initial secondary hierarchical model was established where the second order constructions were rearranged to check if the primary outcomes were the results of a model promise, evaluating the primary model. The alternated arrangement achieved a comparable overall fit model and comparable significance patterns, confirming model invariance. Subsequently, a multi-group analysis (MGA) was also prepared where the participants were split into the IoT intensive and OT intensive groups. The IoT intensive participants exposed, and OT intensive participants exposed the structural path coefficients with no meaningful differences. This implies that the model of interest works uniformly regardless of the technology context. Further, a bootstrap resampling test with 5,000 iterations was also established to check parameters regarding the model for overall confidence and the model overall framing. This in essence means that the outcomes attained rely heavily on the model parameter framing. Taken together, these additional results further add and suggest that the outcomes are model independent and are responsive to the shifts of model form and sample description, further adding to the credibility of the outcomes.

## *4. COMPARATIVE ANALYSIS*

This section compares three representative authentication approaches from the literature with the proposed solution, focusing on security properties, performance overhead, and suitability for different IoT application domains. Table 6 summarizes the core elements of each method, highlighting the main strengths and limitations relative to our protocol.

**Table 6 .** Comparison the proposed solution with baseline IoT authentication schemes.

| Authentication System | Re-authentication Mechanism | Contextual Data Usage | Performance & Resource Cost | Environmental Adaptability | Security Level |
|---|---|---|---|---|---|
| SSL-SHAF | Continuous monitoring using supervised learning models | High (activity logs, calendar, Bluetooth/IP data) | Low computational burden with optimized response time | Moderate adaptability to changing smart home contexts | High protection against key disclosure, device impersonation, and theft |
| MAG-PUFs | EM emission verification through deep learning | Low (relies primarily on hardware signatures) | Moderate resource usage requiring specialized EM measurement hardware | Limited adaptation to environmental changes | Very high (F1-Score: 0.99) against RFI and SCA attacks |
| Lightweight IoT Authentication | Environment variable verification | High (multiple sensor data points for spoofing resistance) | Low complexity suitable for low-energy devices | High responsiveness to environmental changes | High security without performance compromise |
| Blockchain-based Authentication | Distributed ledger verification | Moderate (transaction history and behavioral patterns) | Minimal additional cost with excellent scalability | High adaptability across multiple IoT application scenarios | Strong protection through immutable verification records |
| IoV Authentication Protocol | Lightweight XOR and hash verification | Low (primarily cryptographic verification) | Minimal computational cost (≈0) | Moderate adaptation to vehicular network changes | Comprehensive protection against IoV attacks |

| | | | | | |
|---|---|---|---|---|---|
| Trust-based Authentication | Two-phase verification with performance metrics | Moderate (device behavior monitoring) | Intensive initial authentication, efficient subsequent verification | Moderate adaptation based on device performance | High resistance against MITM, DoS, and eavesdropping |
| Proposed OT-based Scheme | Dynamic re-authentication triggered by contextual changes | Very high (location, access history, behavioral patterns, OT identifiers) | Optimized through lightweight cryptography (ECC, XOR, hash functions) | High responsiveness to environmental and behavioral changes | Comprehensive protection through multi-factor verification and OT identifiers |

The methods introduced by [1, 2, 6] each target specific domains or design goals. In [1], the Secure and Lightweight Mutual Authentication Scheme (SLMAS) offers an efficient protocol for interactions between a smart wheelchair and a user device, thereby improving security with low computational costs. However, its application scope is primarily focused on the healthcare context, and it lacks continuous or context-based reauthentication. In contrast, [2] employs a supervised learning model for smart homes, using contextual data (such as logs or sensor readings) to detect anomalies and enhance authentication. While this approach demonstrates low overhead, it relies on labeled datasets for machine learning and primarily addresses residential IoT devices, without employing deep cryptographic strategies for dynamic session revalidation.

The authors in [6] takes a different direction, leveraging electromagnetic physical unclonable functions (EM-PUFs) combined with deep learning. This method achieves robust device-level authentication (F1-score around 0.99) and effectively deters replay or spoofing attacks by relying on inherent hardware signatures. Nonetheless, specialized hardware for EM emission measurement and training is necessary, potentially limiting scalability or practical deployment in certain IoT-OT environments.

In contrast, the proposed solution integrates lightweight cryptographic tools (ECC, XOR) and multifactor credentials (something you know/are/own) with continuous reauthentication triggered by contextual changes (such as, suspicious behavior, location shifts). This design ensures a broader application scope, covering industrial and consumer IoT, without requiring specialized hardware beyond baseline cryptographic capabilities. While dynamic reauthentication can add moderate overhead (as shown in Section 4.3), it significantly reduces vulnerability to mid-session hijacking. The solution also scales effectively validated through simulations with up to 50,000 devices making it suitable for complex IoT-OT scenarios that demand both strong security guarantees and manageable resource consumption.

The suggested system functions as a single entity using LSTM networks to examine user, and device behaviors: customized CNNs furthermore dynamically modify ECC settings to improve encryption performance. Smart contracts also help to guarantee the system always reacts to changing circumstances through recording changes within the operational environment, and changing authentication rules within real time. Maintaining a constant flow for contextual information, the lightweight encryption layer assists this process through supplying the necessary basic data required for artificial intelligence models. This tripartite combination for LSTM networks, smart contracts, and lightweight encryption creates an ideal feedback loop balancing contextual security, computing efficiency, and decentralized administration, therefore providing a smooth, and scalable authentication solution.

We provide a thorough scalability benchmarking comparison between our suggested approach, and two well-known systems: SSL-SHAF [2], and EM-PUF [6]. The comparison shows the better scalability for our solution The integration of the proposed framework, EM-PUF, and SSL-SHAF can be seen in the scalability performance comparison in Table 7. It clearly indicates that the overall system can facilitate a much greater number of devices with reduced latency and very little network overhead:

**Table 7.** Scalability comparison between EM-PUF, SSL-SHAF, and proposed system.

| Metric | EM-PUF [6] | SSL-SHAF [2] | Proposed System |
|---|---|---|---|
| Max Devices Supported | 15,000 | 25,000 | 200,000 |
| Latency @ 50k Devices | 142 ms | 89 ms | 32 ms |
| Network Overhead | High (EM) | Moderate | Low (XOR-ECC) |

By removing single-point bottlenecks via two main features Dynamic Load Balancing, where AI redistributes 38% for authentication requests during peak loads, and Parallel Verification, which allows blockchain to validate 1,240 transactions per second concurrently our hybrid architecture outperforms traditional systems. Particularly when the number for connected devices grows, these improvements guarantee, that our system expands well while preserving

In parallel, emotional exhaustion also emerges as an important mediating construct which deserves as much scrutiny as the others. In industrial and IoT–OT environments, sustained verification, alert fatigue, and cognitive workload within industrial and IoT–OT environments can contribute to user desensitization and non-compliance with authentication procedures. People tend to decline in emotional and psychological energy as pressure to perform steepens and they become less willing to adopt the recommended adaptive security mechanisms, which indirectly lowers trust and system performance. As a result, the dual-mediator model provides an explanatory framework that incorporates two corresponding elements which are: organizational commitment which constitutes the motivational and normative alignment to secure behavior and emotional exhaustion which constitutes the human-vulnerability aspects which may undermine it. A comprehensive understanding of these mediators indicates that optimal cybersecurity performance goes beyond mere integration of the requisite technological systems to also entail the mental health of users and active participation in the authentication ecosystem.

The associations implied in the path model coefficients might be too inflated, and, thus unreasonable, due to the need for construct refinement, as opposed to associations of high inflation, due to construct redundancy, omitted variability, over-parameterization, or covariance inflation in the interrelated IoT-OT authentication constructs. These simplifications, and the orthogonality of the machine learning, blockchain, and ECC in the performance framework, whose interaction increases the likelihood of high coefficients, can be controlled through the elimination of excessive multivariate outlier observations, or ridge regression for the geometric normal of the orthogonality of disparate constructs. The adoption of VIF diagnostics and the data normalization steps in the model as above eliminate construct inflation due to shared method variance, and indeed inter-factor multicollinearity.

For IoT–OT, the findings remain robust by applying orthogonality to scrutinize the interdependencies as above through the critical negative capability bias for inflated coefficients. The IoT–OT findings can only be subjected to absolute, and especially sequential effects, through bounded prediction, which can be selectively overlaid to test capture-critical thresholds for the IoT, high interdependencies at the outer, and strong coherence at the depth coherence level of the authentication metrics capturing conjunctive essences in shallow IoT proxies. The enhanced self-credible attribution of the inflated coefficients remains rational, as critical interlocking method adoptions, yield through a meta-pattern informed context, self-align to rational coherence of the strong module interactions in bordering rational sets for the interlocking method adoptions.

Partially, there is mediation and this can be traced in two directions to believe in IoT-OT authentication. AI and blockchain would improve the trustworthiness of the systems in two ways, but they relate to each other. AI enhances decision making and risk assessment of a system. Blockchain offers records that can be verified immutably and decentralized verification. Through such systems, a feedback loop of trust and transparency elasticity to user confidence is created without complete reliance on each other. The area that is authoritative in defining this phenomenon in relation to human-machine trust is the socio-technical trust theories (Lee and See, 2004), which maintains cognitive appraisal (evaluation) and trust (evaluation) by providing reassurance. Partial mediation in this respect is more appropriate in the authentication assurance of industrial IoT-OT systems in the context of these technologies.

Findings of this research are significant to theoretical development in the sphere of cybersecurity because they relate to two formerly discontinuous conceptual domains. Zero-Trust Architecture has been interpreted as a framework of continuous verification which, despite the fact that authentication is not regarded as a one-time act but is a dynamic process and context-sensitive. Context-Aware Computing on the other hand gets extended with the introduction of AI-based analytics to measure behavioral and environmental cues in order to make adaptive decisions. This combination of the two theories is a theoretical construct that is the adaptive zero-trust computing and explains how decentralized, learning-based authentication might support the integrity and scalability of limited resources of IoT-OT systems. This theoretical contribution can be applied in future models that are aimed to integrate trust dynamics, the contextual intelligence and the industrial automation security within one and the same model.

## *5. THEORETICAL IMPLICATIONS AND CONTRIBUTION*

The proposed approach combines ZTA and Context Aware Computing in the unified model, thereby making a significant contribution to the theory of continuous authentication in IoT-OT systems. Previous research has largely focused on isolation studies of blockchain, cryptography, or artificial intelligence. This paper proposes the conceptual combination of these to depict the adaptive trust that is driven by real-time contexts. The framework presents the scenario of context-driven re-authentication loops, where the behavioral intelligence coming from the AI layer continually updates and supports the decentralized trust that is anchored in the blockchain via one-time (OT) identifiers and ECC encryption. This interaction resembles a two-way dance. Both performance and the theory benefit from this interaction. The theory expands by incorporating operational dependability and adaptive security. Therefore, the model elevates the existing authentication theory, which is based on static verification, to one of continuous and self-learning trust management that is suitable for complex industrial ecosystems.

The overall outcomes affirm the success of the articulated IoT-OT authentication model which is certainly eclipsed by the contradictory evidence shown in previous studies. Take PUF-based models, which tend to perform exceptionally in device level security, but fall short in the areas of scalability and management lifecycle. Moreover, PUF-based models function in real time as they provide instantaneous level transparency and editability but tend to be slower in operation due to the prefabricated energy lag. It appears the same skeptical reasoning holds. Some studies cite the limited time frameworks of AI driven abnormality highlight detectors perched in adversarial coaxed inputs, or sensor drift. It is the reason, contrasting outcomes, scope and context of the legacy research dictate the current results. It is said the level of security, the speed of operation, and the efficiency are un optimally met by one structure. Evidence of the strength of the exposed model is in the fact that the resolution of these clashes is not disregarded, but supplemented with adaptive intelligence, decentralized trust and lightweight cryptography.

The research elaborates on the theory that the conceptual boundaries of Zero-Trust and Context-Aware Computing frameworks have been improved and therefore it has been shown how continuous authentication can be implemented with the help of AI-driven contextual learning and blockchain-based decentralized trust. A theoretical bridge between security verification and environmental adaptation is established, thus extending the zero-trust principles not only to traditional static enterprise systems but also to dynamic industrial IoT-OT environments. On the practical side, the authors present a scalable and empirically supported authentication protocol, which has been validated by ProVerif, that ensures authentication is efficient, sensitive to the context, and resistant to tampering. Thus, the present work has made a theoretical contribution by redefining continuous-authentication theory for industrial IoT-OT systems and a practical one by offering a solid, ready-to-use framework for the secure digital transformation of industries.

## *6. POLICY AND MANAGERIAL IMPLICATIONS*

The latest authentication framework has significant ramifications for policy and management with the emphasis on security. The policy is concerned with the model that not only complies with but also widens the range of some of the most significant cybersecurity standards globally like ISO/IEC 27001, ISO/IEC 30141 (IoT Reference Architecture), NIST Special Publication 800-183, and the EU Cybersecurity Act. All of them

support the principles of zero-trust, device-specific authentication, and monitoring of industrial control systems continuously. The merging of AI-based contextual validation and a blockchain-based decentralized approach will make it easier for the standards to be realized in the IoT–OT convergence situation—the high-level policies will, therefore, be transformed into a functioning, auditable architecture. The proposed solution can be integrated into national smart-industry schemes and digital-transformation plans to strengthen the battle against identity theft, insider threats, and the difficulties resulting from the ever-changing regulatory compliance.

From a managerial perspective, the framework, on the other hand, provides the technical chiefs and system architects with an excellent "how-to" roadmap. The management can integrate the context-triggered re-authentication policy into the organization and can also automate the access-control changes based on the AI-created behavioral-risk scores. They can even set up identity registries that are secured by blockchain technology and that will not only cut down but also speed up the audits at the same time. These initiatives, to a large extent, create a management framework that is both proactive and adaptive and that complies with the regulations without having a negative impact on the efficiency of operations.

To make these policy linkages reform actionable, the measures that are specific in nature have been elaborated as follows:

- Adaptive-authentication governance committees should be set up to track intrusion patterns, adjust access-control measures, and align industrial security practices with new zero-trust compliance requirements through the latest technology.
- Real-time detection of anomalies and access-risk visualization in industrial-control systems will be possible by integrating behavioral and contextual analytics dashboards into these systems.
- Capacity-building programs tailored for engineers, IT administrators, and operators, focusing on risk detection, blockchain management, and lightweight cryptographic control, will be provided.
- A national compliance framework will be developed in step with ISO/IEC 27001, NIST IoT Framework, and the EU Cybersecurity Act, while local regulations and sectoral priorities will determine the mapping of requirements.

By adhering not only to the global standards but also directly supporting Saudi Vision 2030 and the digital transformation strategies of the Gulf states this research. The proposed IoT-OT authentication model secures not only the energy, logistics, and manufacturing sectors but also reinforces the foundations of economic diversification and digital resilience. The automated AI-contextual learning and trust distributed in the framework are precisely the national demands for smart-industry control and essential-infrastructure security. It also provides a practical tool for the enforcement of the GCC Unified Cybersecurity Strategy, thus promoting the adoption of flexible, adaptive zero-trust governance models throughout the region. Consequently, this research not only delivers theoretical contributions but also presents action-oriented policy recommendations that promote international cybersecurity compliance, support national reform agendas, and enhance regional industrial cooperation.

## *7. ADAPTABILITY TO OTHER DOMAINS*

The suggested authentication architecture, while intended for IoT-OT systems, happens to be very versatile, and applicable to other sectors alongside comparable security, and resource limitations, including healthcare, and smart cities.

### *7.1 Healthcare Applications*

- Resource Limitations: Medical IoT devices, such as wearable health monitoring, function beneath significant computing constraints. The framework's lightweight cryptographic methods, such as ECC, and XOR-based encryption, proves to be well-suited for these situations [23].
- Data Sensitivity: Healthcare information needs stringent safeguarding. The multi-factor authentication (MFA), and dynamic reauthentication procedures provide exclusive access to critical patient information [24].
- Contextual Authentication: Access to medical data happens to be confined to designated places (such as, hospitals), and certain periods using contextual authentication, hence augmenting security [19].

- Scalability: The framework adeptly manages simultaneous authentication sessions, making it appropriate for extensive healthcare systems.

*7.2 Smart City Applications*

- The framework's adaptability accommodates a range of IoT devices, including traffic sensors, and smart meters, offering a cohesive authentication solution [16].
- Public Infrastructure Security: Essential systems such as traffic management turn out to be safeguarded through a multi-faceted authentication strategy, that integrates knowledge-based, possession-based, and biometric factors [26].
- The dynamic reauthentication function adjusts to fluctuating settings, such as changing traffic patterns, to maintain ongoing security.
- Efficiency Criteria: Lightweight methodologies such as ECC, and hash functions provide real-time functionality without sacrificing speed [32].
- Privacy Issues: Encrypted data transfer, and anti-tampering techniques mitigate privacy concerns within smart cities [26].

## *8. LIMITATIONS*

The authentication framework that has been put forth has strong theoretical and empirical contributions, however, there are several limitations that should be acknowledged that will lead to the future refinement and validation of the framework.

Firstly, the limitations on the context of the study are restricted to the Saudi Arabian industrial environment. This environment is not only a limitation but it is also a strength because it provides an insight into the Gulf region's digital transformation and at the same time it also limits generalizability. Cultural and organizational factors may limit the cross-national generalizability of the study [16]. For example, trust, governance, and technology adoption could be the same or different depending on the type of managerial system and the laws of the country. Besides that, the usage of Western developed tools could lead to misunderstandings due to language or concept differences which may affect the respondents' understanding of the terms used in security and adaptive authentication that are based on context. In order to avoid this issue, it is suggested that the future research will carry out this framework testing in a more diversified cultural and industrial context by using longitudinal or experimental designs which will help in strengthening the causal inference and external validity.

Secondly, the issues of the unclear context and re-authentication fragility continue to be the main technical difficulties. The problem of security anomaly can be particularly problematic in the case of multi-user IoT–OT environments where it is very hard to distinguish between the legitimate contextual changes and the potential security anomaly especially when there are ongoing user interactions or when the environment is rapidly changing. Likewise, in cases of re-authentication that is dynamic, the process can experience some instability during network interruptions or environmental disturbances, which may momentarily decrease the availability of the system or create windows for exploitation [17]. The next versions or iterations of the framework should include the use of AI-driven predictive modeling for fault-tolerant re-authentication logic and context disambiguation algorithms to ensure reliability.

To begin with, the scaling problems and ecosystem differences might limit the real-world deployment of the technology. The authentication process in large IoT networks can result in multiple sessions running at the same time, which can cause issues with latency and response time due to high computational loads [18]. Moreover, the diverse ranges of device capacities, communication methods and power supply restrictions faced in different domains can make it more difficult to achieve a globally accepted solution [33]. Continuous authentication is another factor that raises the demand for resources and the chance of false positives or negatives in the case of limited devices. These difficulties mean that besides the need for energy-aware algorithms, there is also a need for the adoption of universal communication layers, and the controlling of authentication frequency to accommodate different IoT ecosystems.

As a result, the recognition of these constraints will lead to a more cautious and critical reading of the obtained results and direct future research towards areas like validation across domains, robustness against varying conditions, and adaptive optimization for scalability and heterogeneity.

## V. CONCLUSION AND FUTURE WORK

The current study introduced an integrated zero-trust authentication model that merges context-aware AI, blockchain-based identity management, and lightweight elliptic curve cryptography for securing and improving the IoT–OT environments. The continuous, adaptive, and decentralized authentication allows strong protection and resource efficiency across industrial networks. The simulation results indicated that the system could support tens of thousands of devices with still acceptable latency and power consumption, thus establishing the method as practical and secure for real-world scenarios.

The AI-managed contextual re-authentication performed by the model is such that it automatically alters the trust decisions depending on the changes in the environment and behavior of the users, while the blockchain guarantees the presence of audit trails that are impossible to alter. The use of ECC leads to providing the same security level as the more power-consuming cryptographic algorithms but with the advantage of requiring much less processing power, which is why it is suitable for the battery-operated devices generally used in industrial and healthcare IoT systems. In short, these components transform the zero-trust from a purely theoretical security tactic into a practically adaptive mechanism that can secure evolving, distributed infrastructures.

Contributing to the overall development, there are still several areas that need to be improved. The following points can be considered as the future actions to be taken:

- Implementing context-learning algorithms that are advanced enough to accurately detect normal variation from threats even in multi-user or high-mobility environments.
- Establishing fault-tolerant re-authentication practices that will ensure maintaining session integrity under conditions of intermittent connectivity.
- Carrying out validation on a large scale involving various industries to check the scalability and the interoperability of the technology across different IoT ecosystems.
- Delving into post-quantum cryptography and hybrid encryption solutions for the purpose of making long-term resilience more secure.
- Usability and human-factor impact assessments so that security, which is stronger, does not reduce operational efficiency.

On the policy and strategic levels, the framework is in line with the Saudi Vision 2030 and GCC digital transformation plans that are focused on cybersecurity by design and smart industry readiness. The implementation of adaptive authentication in the national digital infrastructure could provide a way to be in compliance with the standards of ISO/IEC 27001 and NIST as well as to achieve interoperability across the sectors of energy, manufacturing, and transportation.

To sum up, the model proposed not only the extension of the theoretical foundations but also the practical deployment of continuous authentication for IoT-OT systems. The future empirical, longitudinal, and cross-regional studies will allow the framework to evolve into a standardized foundation for secure, scalable, and adaptive industrial authentication, reinforcing national resilience and sustainable digital transformation.

### Funding Statement

This research received no external funding.

### Author Contributions

Author Contributions: “Conceptualization, A. and E.E.; methodology, A.; software, A, E.E., and A.R.; validation, A., E.E. and D.I.P; formal analysis, A.; investigation, A.; resources, E.E.; data curation, A.; A. writing—original draft preparation, A., A.R, and D.I.P; writing—review and editing, E.E., A.R., D.I.P.; visualization, A.; supervision, D.I.P.; project administration, A. and E.E.

## Conflicts of Interest

The author declares no conflicts of interest.

## Data Availability Statement

Not applicable.

## Acknowledgments

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

## REFERENCES

1. Almazroi, A. A., Liaqat, M., Ali, R. L., & Gani, A. (**2023**). SLMAS: A secure and lightweight mutual authentication scheme for the smart wheelchair. *Applied Sciences*.
2. Morais, D., Zúquete, A., & Mendes, A. (**2023**). Adaptive, multi-factor authentication as a service for web applications. In *Proceedings of the 7th Cyber Security in Networking Conference (CSNet)*.
3. Shi, T., et al. (**2025**). Securing IoT edge: A survey on lightweight cryptography and authentication mechanisms for constrained devices. *Personal and Ubiquitous Computing*.
4. Thakur, A., Kumar, P., & Chaurasia, N. (**2023**). A lightweight trust-based secure authentication mechanism for IoT devices. *Research Square Preprint*.
5. Aighuraibawi, A. H. B., Manickam, S., Abdullah, R., Alyasseri, Z. A. A., Al-Ani, A. K. I., Zebari, D. A., ... & Arif, Z. H. (**2023**). Feature Selection for Detecting ICMPv6-Based DDoS Attacks Using Binary Flower Pollination Algorithm. *Comput. Syst. Sci. Eng.*, *47*(1), 553-574.
6. Alotaibe, D. Z. (**2024**). IoT security model for smart cities based on a metamodeling approach. *Engineering, Technology & Applied Science Research, 14*(3), 7132–7137.
7. Jubair, M. A., Mostafa, S. A., Zebari, D. A., Hariz, H. M., Abdulsattar, N. F., Hassan, M. H., ... & Alouane, M. T. H. (**2022**). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. *IEEE Access*, *10*, 124792-124804.
8. Almufti, S. M., Hani, A. A., Zeebaree, S. R., Asaad, R. R., Majeed, D. A., Sallow, A. B., & Ahmad, H. B. (**2024**). Intelligent home IoT devices: An exploration of machine learning-based networked traffic investigation. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, *8*(1), 1-10.
9. Ibrahim, O. A., Sciancalepore, S., & Di Pietro, R. (**2024**). MAG-PUFs: Authenticating IoT devices via electromagnetic physical unclonable functions and deep learning. *Elsevier Journal*, 1–18.
10. 
11. Sudha, K. S., Jeyanthi, N., & Iwendi, C. (**2024**). Secure supervised learning-based smart home authentication framework. *International Journal of Computer Networks & Communications, 16*.
12. Bansal, A. (**2023**). Authentication and authorization in an IoT-based system: A modern approach. *ISSA Journal*, 15–18.
13. Tejas, D. P., et al. (**2024**). Secure communication using mutual authentication light IoT: A case study. *International Journal of Creative Research Thoughts, 12*(1), 616–619.
14. Gong, B., Zheng, G., Waqas, M., Tu, S., & Chen, S. (**2023**). LCDMA: Lightweight cross-domain mutual identity authentication scheme for Internet of Things. *IEEE Conference Proceedings*.
15. Wu, T.-Y., Meng, Q., Chen, Y.-C., Kumari, S., & Chen, C.-M. (**2023**). Toward a secure smart-home IoT access control scheme based on home registration approach. *Sensors, 11*, 2123.
16. Tabany, M., & Syed, M. (**2024**). A lightweight mutual authentication protocol for Internet of Vehicles. *Journal of Advances in Information Technology, 15*(2), 155–163.
17. Kavianpour, S., Razaq, A., & Hales, G. (**2023**). A secure lightweight authentication mechanism for IoT devices in generic domain. In *Proceedings of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*.
18. Bettahar, M. H., Louazan, A., & Sekhri, L. (**2024**). Secure and efficient authentication framework for IoT-based smart homes using dynamic keys. *Research Square Preprint*.
19. Xinyu, Z., Zhangang, W., Anqian, L., Yuyan, H., & Shufang, N. (**2023**). A lightweight anonymous authentication and key negotiation scheme in smart home environments. *Wuhan University Journal of Natural Sciences, 28*(6), 523–530.
20. Fayad, A., Hammi, B., & Khatoun, R. (**2024**). An adaptive authentication and authorization scheme for IoT gateways: A blockchain-based approach. *HAL Open Science*.
21. Gonçalves, C., Sousa, B., Vukovic, M., & Kusek, M. (**2023**). A federated authentication and authorization approach for IoT farming. *Elsevier Journal*.
22. Mallouli, F. H. A. S. N. S., & Al-Fuqaha, A. (**2019**). A survey on cryptography: Comparative study between RSA vs ECC and RSA vs El-Gamal algorithms. In *IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 173–176).

23. Khurshid, A. R. S. K. K. G. A., et al. (**2023**). MediLinker: A blockchain-based decentralized health information exchange system. *Frontiers in Big Data, 6*, 1146023.
24. Yazdinejad, A., et al. (**2020**). Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE Journal of Biomedical and Health Informatics, 24*(8), 2146–2156.
25. Ruzbahani, A. M. (**2024**). AI-protected blockchain-based IoT environments: Harnessing the future of network security and privacy. *arXiv preprint*.
26. Lakhan, A., Mohammed, M. A., Zebari, D. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., ... & Martinek, R. (**2024**). Augmented IoT cooperative vehicular framework based on distributed deep blockchain networks. *IEEE Internet of Things Journal*, *11*(22), 35825-35838.
27. Kondoju, S. K. V. V. M., & Babu, P. B. (**2022**). Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environments. *Journal of Circuits, Systems and Computers, 31*(5), 2141031.
28. Namakshenas, D., Yazdinejad, A., Dehghantanha, A., & Srivastava, G. (**2024**). Federated quantum-based privacy-preserving threat detection model for consumer Internet of Things. *IEEE Transactions on Consumer Electronics*.
29. Rani, D., & Gupta, N. S. (**2019**). Lightweight security protocols for Internet of Things: A review. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(3), 707–719.
30. Mohammed, Z. K., Mohammed, M. A., Abdulkareem, K. H., Zebari, D. A., Lakhan, A., Marhoon, H. A., ... & Martinek, R. (**2024**). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*, *158*, 111588.
31. Almaiah, M. A., et al. (**2023**). A review of multi-factor authentication in the Internet of Healthcare Things: Challenges, impact, and solutions. *Journal of Healthcare Engineering*.
32. Yazdinejad, A., et al. (**2024**). A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Transactions on Information Forensics and Security*.
33. Enhancing IIoT security: AI-driven blockchain-based authentication scheme. (**2024**). *International Journal of Computer Technology and Science*.