Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/GC03.20260311
Published: February 2, 2026

Enhancing Security in Smart Home/Office Automation Systems Using Smart Contract and Facial Recognition

Nura Ibrahim Alameer
College of Computer Science
King Khalid University, Abha, Saudi Arabia
443800953@kku.edu.sa
Nora.alameer11@gmail.com

Nada Alasbali
Department of Informatics and Computer Systems
College of Computer Science, King Khalid University
Abha 61421, Saudi Arabia
Nalasbali@kku.edu.sa

Ahmad J. Alkhodair
University of Tabuk
Aalkhodair@ut.edu.sa

Abstract

The rapid expansion of Internet of Things (IoT) devices within smart home and office environments has introduced new security challenges, particularly in authentication and access control. Many users, even those with technical expertise, often lack adequate mechanisms to safeguard their privacy against cyberattacks targeting IoT systems. To address these vulnerabilities, this work integrates blockchain technology with facial recognition to provide a secure, reliable, and user-friendly authentication framework. The proposed system employs facial biometric verification alongside Ethereum-based smart contracts to ensure decentralized, tamper-resistant access control. A comprehensive performance and security analysis was conducted to evaluate the system's effectiveness. Experimental results demonstrate that the proposed method offers efficient execution times, low transaction costs, and strong resistance to common cyberattacks, confirming its suitability for protecting IoT devices in smart home and office settings.

Keywords

IoT, Blockchain, Smart Contract, Access Control, Facial Recognition.

1. Introduction

The proliferation of Internet of Things (IoT) devices has significantly transformed multiple sectors—including healthcare, transportation, agriculture, and smart cities—by enhancing convenience, automation, and operational efficiency. However, as IoT systems become more deeply embedded in smart home and office environments, they introduce substantial security risks. Weaknesses in authentication and access control mechanisms remain a primary concern, often exposing critical infrastructure to unauthorized access, manipulation, and data breaches. Ensuring robust, scalable, and privacy-preserving authentication is therefore essential to mitigate evolving cyber threats (Pawar et al. 2018). Prior research emphasizes the urgent need for advanced frameworks capable of addressing these complex and dynamic security challenges (Soni and Singh 2025).

Blockchain technology, combined with smart contracts, has emerged as an effective paradigm for strengthening IoT security. As a decentralized and immutable ledger, blockchain facilitates transparent, autonomous, and verifiable interactions among IoT devices. Smart contracts enforce predefined rules that restrict unauthorized access, preserve data integrity, and minimize the risk of cyberattacks (Giannoutakis et al. 2020). For example, Lin and Yau (2023) introduced a blockchain-based, situation-aware access control model that enhances transparency and protects transaction data. In addition, integrating blockchain with advanced machine learning techniques, such as federated learning, has shown promise in establishing robust, privacy-preserving intrusion detection systems within smart home environments (Shalan et al. 2025).

In parallel, facial recognition has emerged as a highly effective biometric authentication method. By analyzing unique physiological characteristics, facial recognition offers several advantages over traditional password-based authentication, including non-intrusive verification, enhanced accuracy, and improved user convenience. The difficulty of replicating or forging facial features further strengthens its security. Standard recognition techniques extract distinctive facial attributes—such as ocular, nasal, and contour features—and compare them with stored templates for identity verification (Alsellami and Deshmukh 2021).

Despite progress in both areas, an important gap remains: existing systems often fail to integrate decentralized blockchain-based access control with intuitive and secure biometric authentication. Many frameworks either lack comprehensive decentralization or rely on weak or outdated authentication approaches, leaving them vulnerable to sophisticated cyber-physical attacks. This highlights the need for unified solutions that combine strong authentication with decentralized enforcement to improve security, privacy, and resilience in smart environments.

To address this gap, this research proposes an integrated system that enhances smart home and office security through the combined use of facial recognition and blockchain-IoT technologies. The system employs facial biometric authentication backed by secure database verification, along with Ethereum smart contract protocols for decentralized access control. This integration enables authorized users to interact with IoT devices securely and efficiently. Furthermore, this study provides a detailed performance analysis, including execution time and transaction cost evaluation. The remainder of this paper is organized as follows: Section 2 presents related work; Section 3 describes the proposed system; Section 4 discusses the experimental results and validation; and Section 5 concludes the paper and outlines future research directions.

1.1 Project Problem Statement

Most smart home and office devices remain vulnerable to cyberattacks due to weak authentication mechanisms and insufficient protective controls. Even technologically experienced users often lack the necessary tools to secure their devices and safeguard their privacy. These vulnerabilities can be exploited by attackers to compromise sensitive data and disrupt system functionality. The interconnected nature of smart home and office ecosystems further amplifies these risks, enabling attackers to move laterally across the entire network (Ratkovic 2022).

1.2 Solution

Blockchain technology represents one of the most effective approaches for addressing authentication challenges and mitigating cyberattacks in smart home and office environments. Its decentralized architecture provides a robust and tamper-resistant security mechanism, and has been widely recognized for its reliability in securing digital systems (Fotiou and Polyzos 2018). To enhance the security of IoT systems, it is essential to protect device vulnerabilities and prevent malicious activities. The proposed solution integrates facial authentication with Ethereum-based smart contracts, supported by a sensor device and a Raspberry Pi 3 Model B, to ensure secure, reliable, and efficient access control.

1.3 Objectives

- Conduct a comprehensive literature review to identify key challenges, issues, and recent developments related to blockchain-IoT smart home/office automation.
- Implement a secure access control mechanism for IoT devices.
- Propose a practical and robust security framework for smart home and office automation using blockchain and IoT technologies.
- Develop a secure authentication method to protect both users and IoT devices.
- Achieve low-cost transactions and high performance in system operations.

2. Literature Review

2.1 Internet of Things (IoT)

The Internet of Things (IoT) is a rapidly evolving technology that connects devices embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. Due to its widespread adoption in modern life, IoT has attracted significant interest from academia, industry, and research communities. IoT ecosystems consist of both software and physical components, forming interconnected environments that support automation and intelligent services (Qashlan et al. 2020).

Alsellami and Deshmukh (2021) examined recent developments in IoT-based biometric authentication, including iris, facial, fingerprint, voice, and gait recognition, as well as multimodal biometric approaches. Multimodal systems integrate multiple biometric traits—whether behavioral or physiological—to enhance authentication accuracy and robustness against spoofing attacks. By combining several biometric indicators, these systems reduce false acceptance and rejection rates while offering improved security, flexibility, and convenience.

Researchers such as Fotiou and Polyzos (2018) explored the integration of smart contracts within IoT systems, focusing on user–Thing interactions, security requirements, and system design guidelines. Their work emphasizes how smart contracts can enhance security by ensuring transparency, deterministic execution, and tamper-resistant operations, while also highlighting the challenges involved in establishing secure connectivity between IoT devices and blockchain networks.

Qashlan et al. (2020) proposed a smart home framework that incorporates attribute-based access control, smart contracts, and edge computing to strengthen authentication. In this framework, attribute-based access control contracts help mitigate denial-of-service attacks by validating user addresses and associated policies before issuing access tokens. Multiple unauthorized access attempts trigger restrictions or complete denial of access, thereby providing an additional layer of protection.

Zhang et al. (2018) introduced a dynamic IoT access control mechanism that integrates smart contracts with machine learning algorithms to evaluate user behavior. The system architecture includes a judge contract, a registry contract, and multiple access control contracts (ACC). Each ACC monitors subject–resource interactions, detects inappropriate or malicious behavior, and triggers penalties through the judge contract (JC), such as temporary access denial or reinstatement once compliance is verified.

In another study, Zhang et al. (2020) combined the Attribute-Based Access Control (ABAC) model with blockchain-based smart contracts to develop a distributed and reliable access control framework for smart cities. The architecture includes a Policy Management Contract (PMC), a Subject Attribute Management Contract (SAMC), an Object Attribute Management Contract (OAMC), and an Access Control Contract (ACC). The results demonstrated improved security and operational efficiency; however, the framework incurred higher deployment costs compared to traditional ACL-based approaches.

2.2 Blockchain

Blockchain, originally introduced by Satoshi Nakamoto, is a decentralized, distributed, and immutable digital ledger that enables secure and transparent transactions without relying on a central authority. Transactions are recorded in chronologically linked blocks and shared among participating nodes through peer-to-peer networks. Owing to these properties, blockchain has been widely adopted as a foundational technology for enhancing security, trust, and access control in Internet of Things environments (Qashlan et al. 2020, Alblooshi et al. 2018, El-Hajj et al. 2019, Zhang et al. 2018).

2.2.1 Bitcoin

Bitcoin is a decentralized digital currency that utilizes the proof-of-work (PoW) consensus mechanism to validate transactions and append new blocks to the blockchain. In this process, miners compete computationally to solve complex mathematical puzzles, with the successful miner receiving newly generated bitcoins as a reward. Although PoW provides strong security guarantees without relying on intermediaries, it has been widely criticized for its high energy consumption and environmental impact. Nevertheless, Bitcoin remains one of the most influential and widely adopted blockchain-based systems (Alblooshi et al. 2018).

2.2.2 Ethereum 2.0

Ethereum 2.0 introduces a proof-of-stake (PoS) consensus mechanism as a more energy-efficient alternative to the traditional proof-of-work (PoW) model. In PoS, validators are selected to create new blocks based on the amount of cryptocurrency they stake as collateral, which significantly reduces energy consumption while improving scalability. In addition, Ethereum 2.0 adopts sharding to enable parallel transaction processing and enhance network throughput. These architectural advancements have motivated the adoption of Ethereum-based platforms in IoT security applications, particularly for authentication, access control, and secure transaction management (Zhang et al. 2018, El-Hajj et al. 2019).

2.2.3 Smart Contract

The concept of smart contracts was first articulated by Nick Szabo in 1994. A smart contract is a self-executing program deployed on a blockchain that automatically enforces predefined rules once specific conditions are satisfied. Each contract possesses a unique blockchain address through which users initiate and execute transactions. Owing to their decentralized and transparent nature, smart contracts remove the need for centralized authorities and significantly enhance system trust. Ethereum remains the most widely adopted platform for developing smart contracts, primarily using the Solidity programming language. When integrated with IoT ecosystems, smart contracts enable secure, scalable, and tamper-resistant authentication mechanisms—effectively reducing dependence on centralized servers and improving overall system security (Qashlan et al. 2020).

Furthermore, recent research has expanded the role of blockchain in enhancing security within smart environments. For example, Soni and Singh (2025) conducted a comprehensive analysis of blockchain-based security mechanisms for smart home systems, demonstrating how decentralized architectures effectively mitigate vulnerabilities inherent in centralized authentication models. Their findings underscore the advantages of blockchain for secure access management and long-term auditability, while also acknowledging persistent challenges such as scalability constraints and integration complexities within existing IoT infrastructures. These insights are consistent with contemporary research trends that emphasize strengthening authentication and access control through the combined use of blockchain and smart contract technologies.

2.3 Face Recognition

Biometric authentication has gained substantial attention for its accuracy, convenience, and resilience against impersonation attempts. Among the various biometric modalities, facial recognition has emerged as a particularly effective and non-intrusive method for verifying user identity. The authentication process captures an image of the user's face, extracts distinctive features—such as ocular, nasal, and oral characteristics—and compares them against securely stored templates. Unlike password-based methods, facial recognition offers enhanced security because biometric traits are inherently difficult to replicate or steal. Despite ongoing concerns related to privacy and data protection, facial recognition remains a reliable and widely adopted authentication mechanism, especially within IoT-based environments (Alsellami and Deshmukh 2021).

Table 1. Literature Review Summary

No	Researcher/s	Contribution	Pros./Result	Cons./Limitation
1	Alsellami and Deshmuk(2021)	This paper highlights current developments in Internet of Things (IoT)-based biometric authentication.	The authentication can enable develops the end user's quality of life and improves competence	single biometric trait can be compromised if the biometric data is stolen or hacked.Once compromised,the biometric data cannot be changed like a password.

2	Fotiou and Polyzos (2018)	They discussed how smart contracts and blockchain technologies can create solutions for the challenges posed by the Internet of Things (IoT).	They mention several advantages of smart contracts,including Transparencyand Deterministic execution	No security issues in smart contract based IoT.
3	Qashlan et al. (2020)	They proposed an authentication scheme which integrate attribute-based access control using smart contracts with ERC-20 Token (Ethereum Request For Comments) and edge computing to construct a secure framework for IoT devices in Smart home system.	The system achieves securitygoals (confidentiality, integrity, availability) and is able to overcome modification anddenial-of service attacks.	The transaction cost is 1,377,071, which is high, and the execution time takes 40 second
4	Zhang et al. (2018)	They proposed a contract-based smart employment contract consisting of several files. They used the Ethereum smart contract platform to implement ACCs, JC and RC to control access to an IoT system with a desktop computer, a laptop and two raspberry pi3 model B devices.	They succeeded in applying their proposed and detecting the misbehavior.	The time performance of the operation takes increased time to execute
5	Zhang et al. (2020)	The research's suggested framework is an Attribute-Based Access Control (ABAC) framework for smart cities that uses Ethereum smart contracts to manage ABAC policies, attributes of subjects and objects, and perform access control. The framework consists of four smart contracts: Policy Management Contract (PMC), Subject Attribute Management Contract (SAMC), Object Attribute Management Contract (OAMC), and Access Control Contract (ACC).	The proposed framework can improve access control's security and efficiency and enhance safety.	The experiment results demonstratedthat, compared to the ACL- based framework, the system imposes a higher deployment cost.

Table 1. presented earlier in this section, compares various existing blockchain-based solutions for managing access to IoT devices and highlights their respective advantages and limitations. The table identifies common issues in current approaches, such as high transaction costs, limited scalability, and dependence on centralized components that compromise system resilience. In contrast, the proposed system leverages decentralized smart contracts and biometric authentication to overcome these challenges. Overall, the table provides a comprehensive summary of the strengths and weaknesses of existing strategies and clearly positions the proposed solution as a viable and enhanced alternative.

3. Methods

This section describes our suggested solution for implementing a secure access control system that uses the This section outlines the methodology adopted to develop a secure access control system that integrates blockchain technology with decentralized authentication mechanisms. As shown in Figure 1, when a user attempts to access an

IoT device, the system first performs facial recognition to verify the user's identity before granting access to the interface where actions such as opening or closing the IoT device can be requested. This authentication stage is powered by FACEIO, which generates an encrypted facial template and allows identity verification. User profile information and identifiers are stored in Firebase to support session management and system logging.

The interaction between the facial authentication module and the IoT device is managed through a blockchain-based smart contract. The smart contract enforces access policies and ensures that no unauthorized user can control the device. The Polygon (Matic) Test Network was selected for deployment due to its low transaction fees and high throughput, making it suitable for real-time IoT applications.

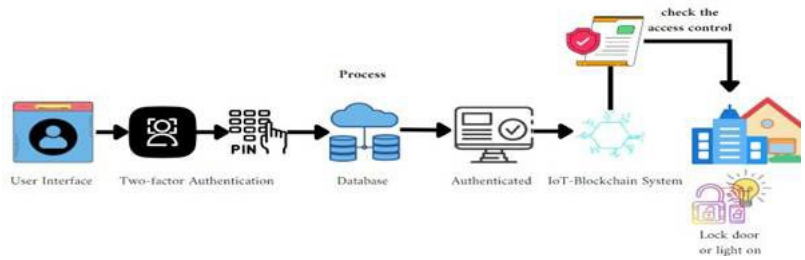

Figure 1. Proposed Solution

3.1 Experimental Setting

The experimental setup employed multiple programming languages—including JavaScript, Python, Solidity, and React JS—to develop a functional prototype for securing smart home and office automation systems. System development was carried out using Remix IDE and Visual Studio Code (VS Code), while the Truffle framework facilitated the deployment and testing of smart contracts.

The Polygon (MATIC) Test Network was used to simulate Ethereum functionality with reduced computational cost. Web3.js and MetaMask wallet were utilized to interact with the Ethereum Virtual Machine (EVM) and the deployed smart contracts. Bootstrap CSS was used for user interface design, and Firebase served as the system's real-time cloud database.

A Raspberry Pi 3 Model B, paired with a sensor module, was employed to collect real-time device data. A smart contract received this data from the Raspberry Pi and validated it before storing it on the blockchain. This design ensured the confidentiality, integrity, and tamper resistance of all stored information.

3.2 Methodology

Data collection and system integration were carried out using several coordinated techniques, described as follows:

3.2.1 Authentication

This study integrates the FACEIO authentication service, which generates an encrypted facial template during enrollment. FACEIO does not store raw facial images or user credentials; instead, it generates a secure facial template used exclusively for identity verification. Complementary user information (first name, last name, and user ID) is stored in Firebase, which supports user session management and record keeping.

The integration process involved setting up the Firebase project, developing the web interface using JavaScript and HTML, and integrating the FACEIO API to manage facial enrollment and authentication workflows. The public application ID provided by FACEIO is required to initialize the authentication process and link the system to the FACEIO service.

- **Registration :** First, users must visit the web interface and create an account by registering their first and last names and opening the camera to take the face information. The FACEIO library will identify the face and then provide us with the user ID, which will be saved along with the user's name information in the Firebase database. From the SignUp file, we have the handleSubmit function and have code, as shown in Figure.2. First, enroll,

responsible for opening the camera to take the face data and the first and last name, take the face ID, and transmit addDoc(collection(db, 'users') and save them in the firebase.

Figure 2. SignUp file

- **Login :**The login button has a handleFaceSignIn function and an authentication process, as shown in Figure.3; in it, there is an authentication process from FACEIO that will fetch data from a collection (db, 'users') in the firebase, and its name is users. This function will ensure that the user is present in the firebase, and it will move it to the session and save it if it exists.

Figure 3. Login file

3.2.2 Smart Contract

To create the smart contract, we used the contract-oriented programming language **Solidity**, deployed it, and verified its functionality using the Matic Testnet platform supported by the Polygon network. The **IOTDeviceControl** smart contract functions as a self-executing agreement recorded on the Ethereum blockchain. It is designed to regulate access to an Internet of Things (IoT) device by automating predefined terms and conditions, thereby enhancing efficiency, security, and transparency in access management—an approach aligned with the capabilities highlighted in prior blockchain-based IoT security research (Fotiou and Polyzos 2018).

The smart contract contains several functions that enable creating and managing user accounts, access levels, and device control. An administrator owns the contract, the only party with authority to create or modify user accounts and access levels. The contract also includes a time-lock feature that allows the administrator to control the time the device can be operated.

Figure 4. createUser function

Figure.4 shows the createUser function that allows the administrator to create user accounts by specifying their Ethereum address and access level. The accessLevel variable is an integer that determines the user's access level to the device. Users with an access level greater than 0 can operate the IOT device.

```
function updateAccessLevel(
    address _userAddress,
    uint _accessLevel
) public onlyAdmin {
    users[_userAddress].accessLevel = _accessLevel;
}
```

Figure 5. updateUser function

The updateAccessLevel function, as shown in Figure.5, allows the administrator to modify the access level of an existing user account.

```
function checkUserDeviceAccess() public  view returns (bool){
   require(timeLock!=false,"Time of Work Done");
      require(
            users[msg.sender].accessLevel >= 1,
            "User does not have sufficient access level to control the device."
          );
```

Figure 6. checkUserDeviceAccess function

Figure.6 displays. The checkUserDeviceAccess function controls access to the device. It checks whether the current time is within the time-lock period and whether the user has sufficient access level to operate the device. If the conditions are satisfied, the code to control the IoT device is executed.

```
function openCloseLockTime()   public onlyAdmin returns(bool) {
    timeLock = !timeLock;

    return timeLock;
}
```

Figure 7. openCloseLock function

The openCloseLockTime function presented in Figuren7 sets the time-lock period during which the device can be operated. The function takes an argument specifying the number of hours the device should be operable. The time-lock period is recorded in milliseconds and is added to the current timestamp to determine the end time of the period. The function toggles the timeLock variable, which controls access to the device during the specified time-lock period.

```
   function deleteUser(address _userAddress) public onlyAdmin {
       delete users[_userAddress];
   }
}
```

Figure 8. deleteUser function

The delete user function in Figure.8 allows the administrator to delete user accounts from the system. The administrator can only call this function and remove users who are no longer authorized to operate the device.

3.2.3 Decentralize IoT Blockchain System Webpage

This page has two buttons for opening and closing the device. When a user clicks open, the command is sent to the can0penTheDoor function and sent to the checkUserDeviceAccess function responsible for contacting checkUserDeviceAccess when they click on open the door. The process is then carried out after that smart contract sends the result to the function handleButtonClick("on") in charge of sending it to the Raspberry Pi. Furthermore,

this instruction will be sent to the canCloseTheDoor function if the user wants to turn the device off. Additionally, it will connect with the (checkUserDeviceAccess) function in the smart contract, and if the user has permission to turn off the device, it will send true. The handleButtonClick("off") function will then receive a Reply to Raspberry message and carry out the instruction, all operations shown in Figure.9 and Figure.10, and finally, Figure.11 displays the execution of the codding in the raspberry pi3.

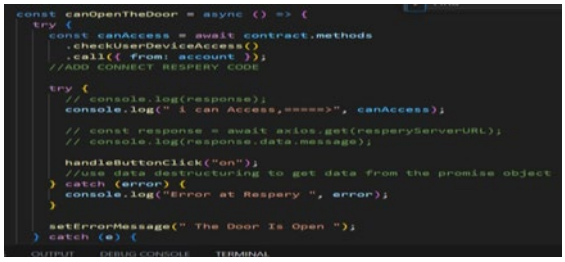

Figure 9. canOpenTheDoor

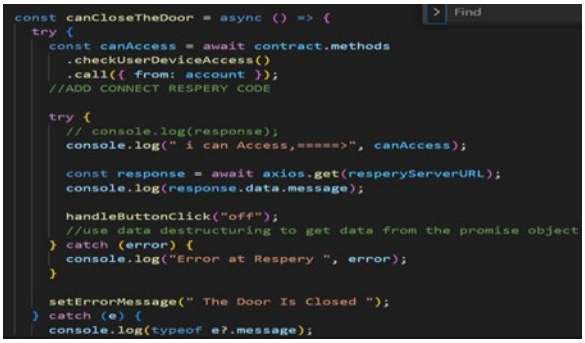

Figure 10. canCloseTheDoor

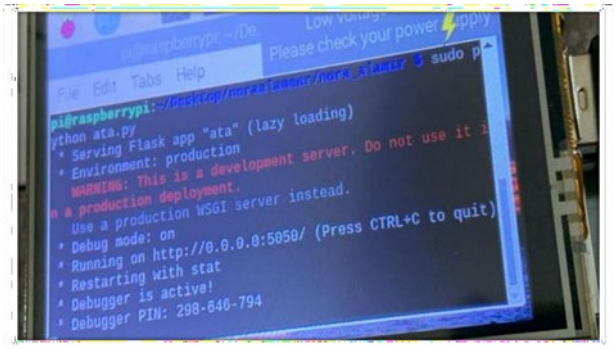

Figure 11. Execution of the code

The following steps describe how to use our system:

Before proceeding to the steps, a necessary step for implementing the project is to deploy the smart contract in Remix IDE, as displayed in Figure.12.

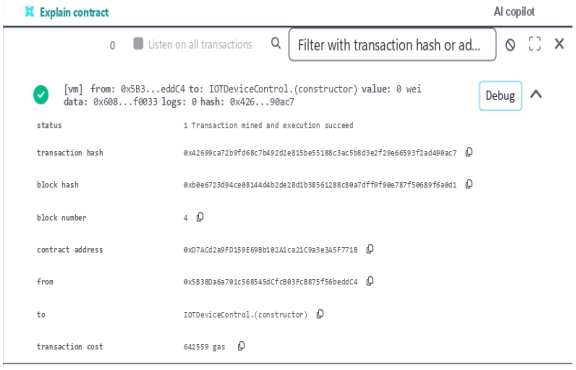

Figure 12. Deployment of the Contract

- **Homepage :**As shown in Figure.13, This user interface is where users must register and log in.

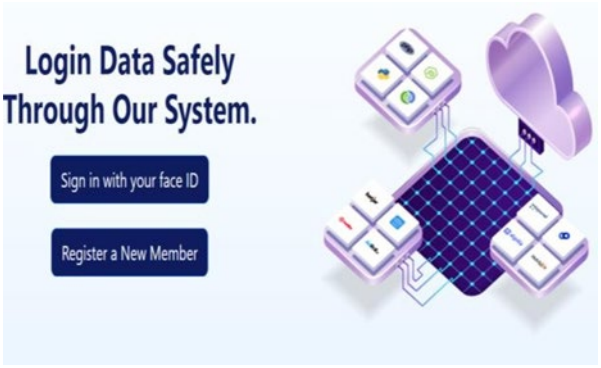

Figure 13. Homepage

- **Register Page :**The Registration button on the Homepage leads to registration, where users must register by inserting their First and Last Name in Figure.14, providing a face ID through FACEIO as shown in Figure.15, creating a PIN code as shown in Figure .16, and then saving their information in the database (Firebase).

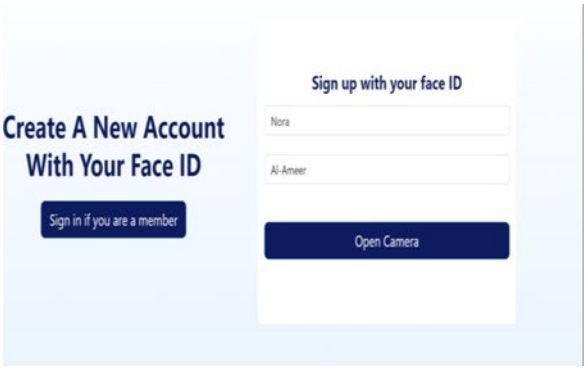

Figure 14. Register Page

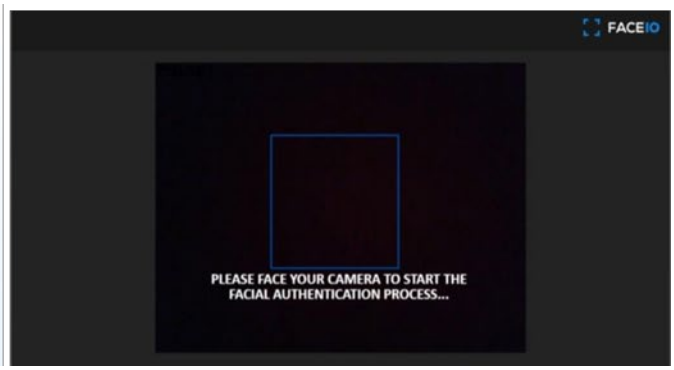

Figure 15. Taking Face ID

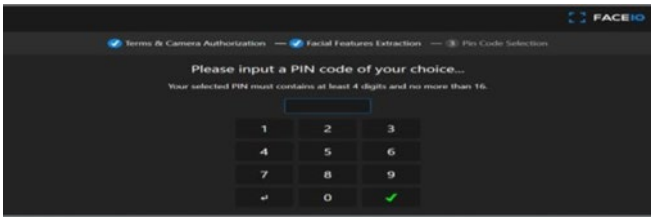

Figure 16. InsertPINCode

- **Login Page :**The login button on the Homepage leads to logging in, where users must log in by Face ID and PIN Code, as we showed before. After which, they can log in and proceed to the next page.

- **IoT Blockchain System :**Metamask enables an administrator to grant a designated user control over an IoT device. However, the administrator must also add this user in the Remix IDE by adding the user account in the function(createUser), as shown in Figure.17.

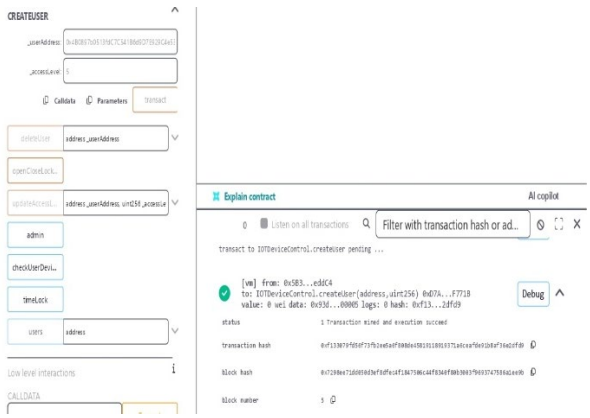

Figure 17. Add User

The presented Figure.18 depicts an unavailability of working time for individuals needing more authorization to enter and control Internet of Things (IoT) devices during permitted hours. This screen is displayed to prevent unauthorized access to IoT devices during restricted periods. The use of such security measures serves to enhance the protection of IoT systems and their associated data.

Figure 18. Unavailable Working Time

- **Admin:** Upon successful login by the administrator, a Dashboard interface will be shown, enabling the modification of the device's status to unlock it, as presented in Figure.19 and Figure.20. However, access to Internet of Things (IoT) devices remains unallowed to unauthorized individuals.

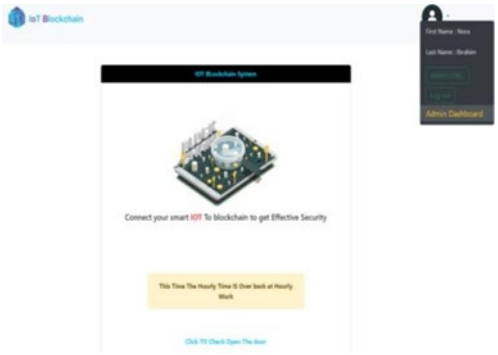

Figure 19. List which Dashboard

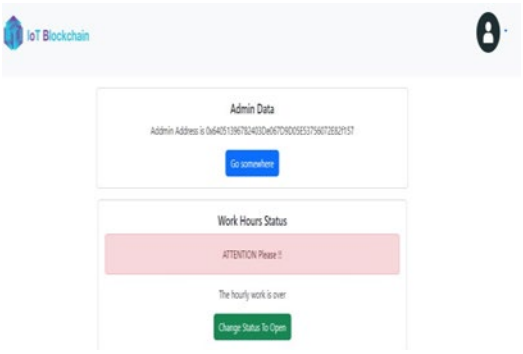

Figure 20. Admin Page

- **Users:** Figure.21 displays a user interface accessible to authorized personnel to control Internet of Things (IoT) devices during specified business hours. Within this interface, authorized users are given the ability to manipulate the status of the door by either opening or closing it. Providing these access privileges to authorized personnel enhances the efficiency and effectiveness of IoT device management during business hours. Figure.22 and Figure 23 show the successful execution of the request, and if unauthorized, trying to access the IoT device will be unallowed to unauthorized. It will display a notification, as presented in Figure.24.

Figure 21. User interface accessible

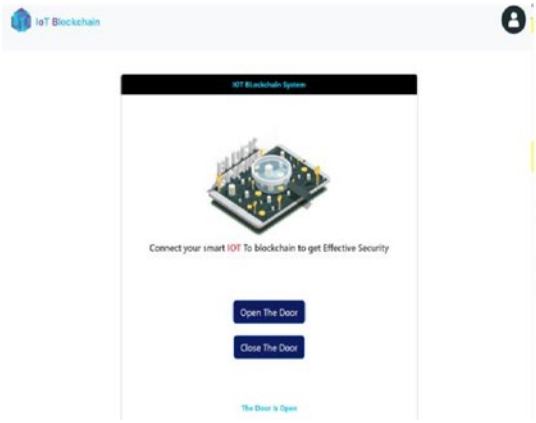

Figure 22. Execute the request

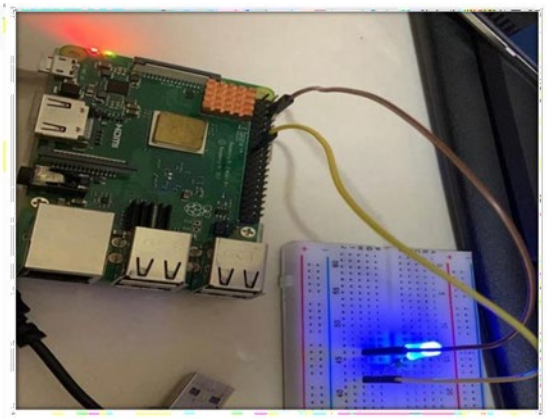

Figure 23. The door is open

Figure 24. Notification

4. Results and Discussion

This section will demonstrate the study's security and present the evaluation findings of the system's development's cost and performance outcomes. In this study, we evaluated the transaction cost of various operations related to enhancing security in smart home/office automation systems using smart contracts and facial Recognition.

4.1 Graphical Results

4.1.1 Cost Analysis

In this study, the transaction cost of several blockchain operations was evaluated to assess the efficiency of the proposed smart home/office security system. All costs were measured in Matic—the native token of the Polygon network—with their equivalents in USD calculated based on the gas price at the time of execution.

The results show that the deployment operation incurred the highest transaction cost, reaching 0.001631811 Matic ($0.0014). In contrast, the createUser operation recorded the lowest cost at 0.00017228 Matic ($0.00014). Both openCloseLock and updateUser demonstrated similarly low costs of 0.00006767 Matic and 0.00007366 Matic, respectively (approximately $0.000054 each). The deleteUser operation required 0.000856 Matic ($0.000072), while changeStatusToOpen incurred 0.00010151 Matic ($0.00009). Overall, the findings indicate that all operations were executed at consistently low costs, highlighting the cost-effectiveness of the system. This efficiency is largely attributed to the Polygon network's reduced gas fees compared to other blockchain platforms. Additionally, the integration of smart contracts with facial recognition minimized the computational overhead by automating core processes, thereby reducing both manual intervention and overall transaction expenses.

Table 2. Comparison of deployment transaction

Contract	**Cost in USD**
IoTDeviceContract	$0.0014
DeviceContract [14]	$3.14

Table 2 shows the transaction cost of deploying the smart contracts used by our system and another research (Valentin et al. 2021). Additionally, it indicates that our system contract's cost is less than other contracts.

Table 3. Transaction cost of DeviceContract

DeviceContract [14]	
Function	Cost in USD
registerDevice	$0.020
unregisterDevice	$0.04
addCompitapleApp	$0.12
setDeviceAddress	$0.07
setDeviceBlockchainAddress	$0.05

Table 4. Transaction cost of IoTDeviceControl

IoTDeviceControl	
Function	Cost in USD
createUser	$0.00014
openCloseLock	$0.000054
updateUser	$0.000054
changeStatusToOpen	$0.000072
deletUser	$0.00009

Tables 3 and 4 show the cost of operations in our research and the other system. As it is apparent in Table 2, the cost of our operations is minimal compared to the system in (Valentin et al. 2021), and this is an advantage of our system; the reason is that we use the Matic Polygon Test Network, whereas the other system used the Ropsten Ethereum Testnet.

4.2 Validation

4.2.1 Time analysis

The performance of our system depends heavily on the execution time of the transactions. The service execution time consists of the time needed to make a transaction request and the web client's confirmation. In addition, the system effectively adds new users and manages access to the smart lock.

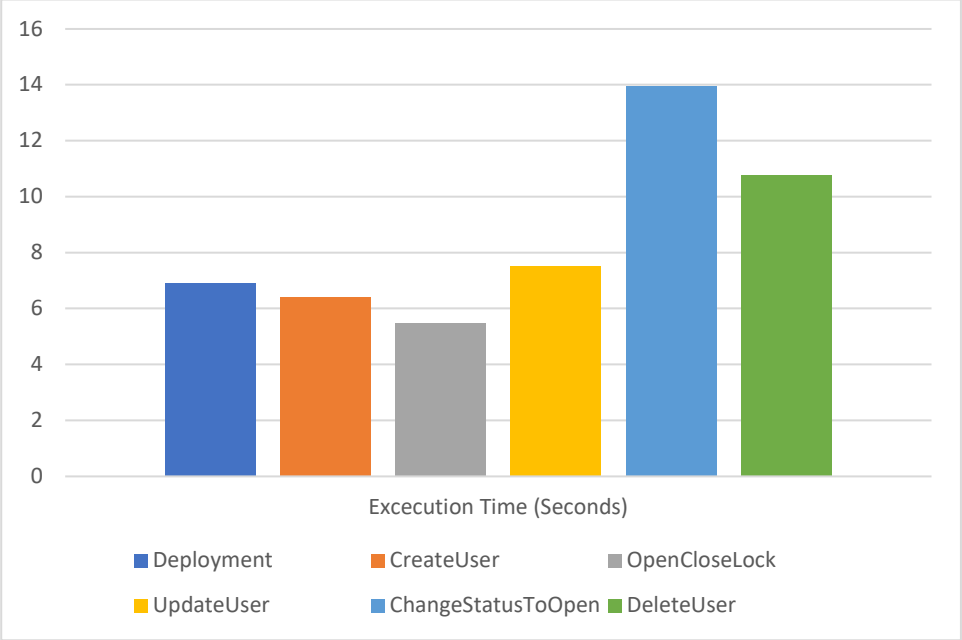

Figure 25. Time Performance

As illustrated in Figure 25, the time-performance evaluation covered six core operations: Deployment, CreateUser, OpenCloseLock, UpdateUser, ChangeStatusToOpen, and DeleteUser. The measured execution times ranged from 5.47 s to 13.97 s, demonstrating a stable and predictable performance pattern across the system. The **OpenCloseLock** operation exhibited the shortest execution time (5.47 s), indicating minimal processing overhead during lock-state interactions. Conversely, **ChangeStatusToOpen** recorded the longest delay (13.97 s), primarily due to the additional blockchain verification steps required before updating the lock status. The remaining operations showed consistent latency values, with **CreateUser** at 6.42 s, **Deployment** at 6.90 s, **UpdateUser** at 7.50 s, and **DeleteUser** at 10.75 s. Collectively, all operations were executed within sub-14-second intervals, confirming the system's overall efficiency, responsiveness, and suitability for real-time IoT environments.

4.2.2 Security Analysis

This section presents the security measures achieved by the proposed system and evaluates its effectiveness in protecting IoT devices and user accounts against various cyber threats. The analysis demonstrates how blockchain technology, smart contracts, and biometric authentication collectively strengthen the system's resilience.

- **Data Tampering:** The decentralized nature of blockchain ensures that stored data cannot be altered without authorization. Smart contracts enforce predefined rules, preventing any unauthorized modification of information once it is recorded on the ledger.

- **Data Breaches:** Because blockchain does not rely on a centralized storage architecture, the risk of large-scale data breaches is significantly reduced. Furthermore, smart contract–based access control restricts data access to authorized users only, thereby minimizing exposure to unauthorized entities.
- **Denial of Service Attack:** Decentralization also enhances system availability by distributing data across multiple nodes. Even if one node becomes unavailable, other nodes continue to operate, preventing service disruption and reducing the impact of DoS attacks (Javaid et al. 2018).
- **Reply Attack:** Replay attacks are mitigated through blockchain's verification and mining processes. Each transaction is validated and stored as a unique entry within the distributed ledger, ensuring that identical transactions cannot be retransmitted or executed more than once (Abubakar et al. 2022).

4.2.3 Biometric Data Retention Policy

The proposed system adopts a privacy-preserving biometric data policy. No raw facial images are stored at any stage. During enrollment, FACEIO generates an encrypted facial template used solely for authentication. This template is retained only while the user is actively registered and is permanently deleted once the user account is removed. Importantly, Firebase does not store or process any facial data. This approach ensures strong protection of sensitive biometric information and minimizes risks associated with long-term data retention.
The study further demonstrates that the proposed system successfully achieves the four fundamental security objectives essential for securing IoT environments:

- **Availability:** The blockchain-based smart contract automates access control processes, ensuring that authorized users can access IoT devices at any time. The decentralized architecture prevents single points of failure, thereby maintaining continuous system availability.
- **Privacy:** Decentralized smart contracts enhance privacy by eliminating the need for centralized storage of user or device data, reducing the likelihood of targeted attacks. Sensitive information is distributed and securely validated across multiple nodes, preventing unauthorized entities from accessing private data.
- **Integrity:** Smart contracts enforce strict rules that prevent unauthorized modification of stored data. Because blockchain records are immutable, malicious actors cannot alter IoT device data without detection, ensuring the integrity of all recorded transactions and operations.
- **Confidentiality:** is maintained through blockchain's inherent access control mechanisms, which ensure that only authenticated and authorized users can view or interact with IoT device information. This prevents exposure of sensitive data to unauthorized parties.

Collectively, these outcomes confirm that the proposed system provides a high level of security and resilience against various cyberattacks targeting IoT environments. In addition to the strong security guarantees, the system also achieves exceptionally low transaction costs and efficient execution times, further demonstrating its practicality, scalability, and overall effectiveness.

4.3 Proposed Improvement

For future work, several promising directions are identified to further enhance the capabilities of the proposed system and address emerging challenges in smart home and office automation. One potential avenue involves integrating advanced machine learning techniques—such as federated learning—with blockchain to develop more robust and privacy-preserving intrusion detection systems, building upon recent research in this area (Shalan et al. 2025). Another direction focuses on exploring cutting-edge artificial intelligence models, particularly vision transformers, and examining how their combination with blockchain technologies can strengthen security performance and improve overall system efficiency (Jan et al. 2025).

A critical next step will be transitioning from the currently used centralized Firebase database to a decentralized storage solution for managing sensitive user and device information. This shift is expected to significantly improve data resilience, enhance privacy, reduce reliance on third-party infrastructure, and eliminate single points of failure. Additionally, future efforts will involve refining authentication mechanisms on the blockchain network and incorporating more sophisticated access-control logic into smart contracts to strengthen protection against unauthorized interactions. Collectively, these advancements aim to prepare the proposed system for large-scale deployment and facilitate its adaptation to real-world IoT environments.

5. Conclusion

This study successfully developed a secure access control system for Internet of Things devices by integrating blockchain-based smart contracts with facial recognition for user authentication. By minimizing the amount of required user data, the system provides strong privacy protection while maintaining high authentication reliability. The comprehensive evaluation of cost and performance further demonstrated the effectiveness of the proposed framework in enhancing IoT security.Quantitative results showed that all key operations were executed efficiently, with execution times consistently below 14 seconds. The fastest operation, OpenCloseLock, completed in 5.47 seconds, while the most time-intensive operation, ChangeStatusToOpen, required 13.97 seconds. These findings confirm the system's ability to maintain secure, responsive communication between IoT devices and blockchain components. In addition, the cost analysis revealed that the proposed system achieves significantly lower transaction fees compared to traditional IoT–blockchain solutions, largely due to the use of the Polygon Matic network.Overall, the results validate the system's efficiency, scalability, and security, highlighting its potential as a practical and cost-effective solution for safeguarding smart home and office environments.

References

Abubakar, M., Jaroucheh, Z., Al Dubai, A. and Liu, X., A lightweight and user-centric two-factor authentication mechanism for IoT based on blockchain and smart contract, Proceedings of the 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pp. 91–96, 2022. https://doi.org/10.1109/SMARTTECH54121.2022.00032

Alblooshi, M., Salah, K. and Alhammadi, Y., Blockchain-based ownership management for medical IoT (MIoT) devices, Proceedings of the 2018 International Conference on Innovations in Information Technology (IIT), pp. 151–156, 2018.https://doi.org/ 10.1109/INNOVATIONS.2018.8606032

Alsellami, B. M. and Deshmukh, P. D., The recent trends in biometric traits authentication based on Internet of Things (IoT), Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1359–1365, 2021. https://doi.org/10.1109/ICAIS50930.2021.9396007

El-Hajj, M., Fadlallah, A., Chamoun, M. and Serhrouchni, A., Ethereum for secure authentication of IoT using pre-shared keys (PSKs), Proceedings of the 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1–7, 2019. https://doi.org/10.1109/WINCOM47513.2019.8942487

Fotiou, N. and Polyzos, G. C., Smart contracts for the Internet of Things: Opportunities and challenges, Proceedings of the 2018 European Conference on Networks and Communications (EuCNC), pp. 256–260, 2018. https://doi.org/10.1109/EuCNC.2018.8443212

Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K. and Nijdam, N. A., A blockchain solution for enhancing cybersecurity defence of IoT, Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), pp. 490–495, 2020. https://doi.org/10.1109/Blockchain50366.2020.00071

Jan, S., Syed, T. A., Alqahtany, S. S., Iqbal, S., Khan, I. and Musa, S., Integrating IoT, blockchain, and vision transformers for enhanced security and efficiency in smart home and healthcare systems, Proceedings of the 2025 4th International Conference on Computing and Information Technology (ICCIT), pp. 145–159, 2025.
https://doi.org/10.1109/ICCIT63348.2025.10989395

Javaid, U., Siang, A. K., Aman, M. N. and Sikdar, B., Mitigating IoT device-based DDoS attacks using blockchain, Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 71–76, 2018.
https://doi.org/10.1145/3211933.3211946

Lin, Z. and Yau, S. S., A blockchain-based approach to improving smart home security with situation-aware access control, Proceedings of the 2023 IEEE International Conference on Blockchain (Blockchain), pp. 340–347, 2023.
https://doi.org/10.1109/Blockchain60715.2023.00059

Pawar, S., Kithani, V., Ahuja, S. and Sahu, S., Smart home security using IoT and face recognition, Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1–6, 2018. https://doi.org/10.1109/ICCUBEA.2018.8697695

Qashlan, A., Nanda, P. and He, X., Security and privacy implementation in smart home: Attribute-based access control and smart contracts, Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 951–958, 2020. https://doi.org/10.1109/TrustCom50675.2020.00127

Ratkovic, N., Improving home security using blockchain, International Journal of Computations, Information and Manufacturing (IJCIM), vol. 2, no. 1, 2022. https://doi.org/10.54489/ijcim.v2i1.72

Shalan, M., Hasan, M. R., Bai, Y. and Li, J., Enhancing smart home security: Blockchain-enabled federated learning with knowledge distillation for intrusion detection, Smart Cities, vol. 8, no. 1, 2025. https://doi.org/10.3390/smartcities8010035

Soni, S. and Singh, A., Analyzing blockchain technology for enhancing security in smart home systems: Current developments and future directions, Proceedings of the 2025 3rd International Conference on Disruptive Technologies (ICDT), pp. 1331–1336, 2025. https://doi.org/10.1109/ICDT63985.2025.10986551

Valentin, M., Pahl, C., El Ioini, N. and Barzegar, H. R., A blockchain-based access and management system for IoT devices, Proceedings of the 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 1–8, 2021. https://doi.org/10.1109/IOTSMS53705.2021.9704951

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. and Wan, J., Smart contract-based access control for the Internet of Things, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2018. https://doi.org/10.1109/JIOT.2018.2847705

Zhang, Y., Yutaka, M., Sasabe, M. and Kasahara, S., Attribute-based access control for smart cities: A smart-contract-driven framework, IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6372–6384, 2020. https://doi.org/10.1109/JIOT.2020.3033434

Biographies

Nura Ibrahim Alameer received her B.S. degree in Information Systems (with honors) from Jazan University, Jazan, Saudi Arabia, in 2018, and her M.S. degree in Information Security (with honors) from King Khalid University, Abha, Saudi Arabia, in 2023. She has academic collaboration experience at Jazan University and the Saudi Electronic University. Her background includes foundational experience in digital forensics, incident response, governance, risk and compliance (GRC), IoT, blockchain, and risk management.

Dr.Nada Alasbali received the B.S. degree in information systems from the King Khalid University, Abha, Saudi Arabia, the M.S. degree in information systems from the University of New South Wales, Sydney, Australia, and the Ph.D. degree in Computer Science and Information Technology with concentration on Internet of Things from the University of Malaya, Kuala Lumpur, Malaysia. Nada's areas of interest are IoT, Smart Systems, Blockchain and smart cities technologies.

Dr.Ahmad Alkhodair received the B.Sc. degree in Computer Engineering from Fahd Bin Sultan University, Tabuk, Saudi Arabia, in 2012 (with honors); the M.Sc. degree in Computer Engineering from the University of Denver, USA, in 2017, and the Ph.D. degree in Computer Engineering from the University of North Texas, USA, in 2023. Since 2012, he has been with the University of Tabuk, where he is currently an assistant professor in computer engineering. He has been involved in several institutional roles related to risk and business continuity and leads a technical initiative on AI-driven resilience analytics. His research interests include cyber-physical and resilient systems, distributed-ledger technologies and their applications, AI for smart cities, and governance–risk–compliance frameworks for digital transformation.