Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Hybrid smart IoT detection and prevention framework for smart cities using blockchain technology

Ahmed Albugmi *

Computer and Information Technology Department, The Applied College, King Abdulaziz University, Jeddah, Saudi Arabia

ARTICLE INFO

Article history:
Received 12 November 2024
Received in revised form
1 March 2025
Accepted 21 April 2025

Keywords:
Smart city security
IoT framework
Blockchain integration
Real-time monitoring
Cyber threat prevention

ABSTRACT

The Internet of Things (IoT) and the development of smart cities provide significant opportunities to enhance security and public safety. However, the increasing complexity of smart city technologies makes them more vulnerable to cyber threats. To address this challenge, this study proposes a Hybrid Detection and Prevention IoT Framework (HDPIoTF) based on blockchain technology. The framework integrates IoT and blockchain to ensure a secure and efficient smart city system through six key stages: IoT sensor development, IoT gateways, blockchain networks, smart contracts, security analytics, and real-time notifications. Using design science as the analytical approach, this study aims to enable real-time monitoring, enhance security, automate responses, and improve interoperability. By leveraging blockchain and IoT, the proposed framework strengthens the protection of critical infrastructure while promoting public well-being.

1. Introduction

Generally, a smart city is defined as an urban area that uses digital technology to collect data and operate/provide services (Buyannemekh and Cook, 2023). Data can be collected from citizens' devices, buildings, and cameras. Traffic and transportation systems are commonly used to facilitate this kind of traffic and transportation system, but there are also several other uses for this technology, including power plants, utilities, urban forestry, water supply and waste disposal systems, criminal investigation systems, and information systems. Additionally, schools, libraries, hospitals, and other kinds of community facilities are also commonly utilizing this technology. Smart cities are places where people, technology, and processes are integrated (Adel and Alani, 2024). They connect and interconnect with other sectors such as the healthcare sector, transportation sector, educational sector, infrastructure sector, etc.

This study aims to develop a hybrid smart detection and prevention IoT framework for smart cities using blockchain technology, called HDPIoTF. This framework aims to leverage the power of blockchain to secure and ensure the reliability and validity of smart city data. Additionally, it aims to implement advanced detection algorithms to detect anomalies and prevent cyber-attacks on IoT devices. Blockchain technology presents a secure and decentralized architecture for data storage and processing.

The remaining parts of this paper are organized as follows: Section 2 discusses related works, the problem statement and research objectives. Section 3 explains the methodology used in this study. Sections 4 and 5 offer validation results and discussion. Finally, Section 6 introduces the conclusion and recommends future research

2. Related works

In the literature, plenty of papers have been written on the security of IoT in smart cities and its applications. For example, Martins (2018) proposed establishing a "mini laboratory," consisting of a wide range of small devices with various interaction capabilities. Several sensors can be found on these rooted devices that can gain data from the temperature, humidity, and light conditions they live in. The authors discussed that several small devices or platforms can be securely communicated with each other and how this can be accomplished.

Authentication and authorization solutions for the Internet of Things were examined in detail by Muzammal and Murugesan (2020) when reviewing centralized as well as decentralized solutions.

* Corresponding Author.
Email Address: analbogome@kau.edu.sa
https://doi.org/10.21833/ijaas.2025.04.013
Corresponding author's ORCID profile:
https://orcid.org/0009-0004-7336-4750

Furthermore, they provided IoT security, and they discussed Blockchain technology and its potential in the IoT era.

Mohammad and Abdulqader (2020) reviewed existing research on cyber security requirements for smart cities. In addition, a few new security requirements were introduced because of the gaps that persist because of the security gaps.

Chaabouni (2020) explained that the use of machine learning as a method of protecting IoT systems would be a highly effective way of detecting and preventing intrusions as early as possible.

Mudawi (2020) suggested a framework for the protection of smart homes. It consists of several matching engines that work together to provide protection. As a result of anomaly-based detection, the IDS/IPS examines all traffic in the home network and identifies, alerts, and/or blocks packets that are detected based on the anomaly detection mechanism.

A secure and reliable method of managing trust and authentication was presented by the authors in Asif et al. (2022). A blockchain-based mechanism is proposed. It is also proposed that smart city resources can be secured using blockchain-based security mechanisms. Moreover, a hybrid application is developed to provide the user with an easy-to-use interface for heterogeneous technologies that are part of the smart city environment.

According to Mohammad et al. (2022), an enhanced authentication and authorization framework has been developed for the Internet of Things. The IoT device side has been developed with an identity verification mechanism that evaluates time stamps for establishing identity, which eliminates the essential for limited uniqueness authentication approaches by using token verification and uniqueness confirmation features built into the token.

An analysis carried out by Rao and Deebak (2022) concluded that security and privacy concerns are mainly a matter of verification methods and key agreements that are used as a basis for the evaluation of multi-criteria verification methods like two-factor multiple-factor verification and three-factor. It has been suggested by the study that these key agreements and verification procedures perform an important part in the evaluation.

Bhardwaj et al. (2022) proposed a novel threat model framework for analyzing Industrial Internet of Things (IIoT) application attacks that have been derived from research. According to the authors, sensitive data flows in IIoT devices could be a source of privacy risks. It was also explored whether it would be possible to exchange devices physically.

Khalil et al. (2022a) reported that authentication mechanisms can be classified as either a type of architecture or a type of method. Smart devices with IoT capabilities were discussed as part of the workshop. As well as analyzing and examining the study's findings, we also applied computation costs, communication overheads, and robustness models to the literature schemes.

According to Fei (2022), the authors have developed an IoT gateway that is safe, secure, efficient, and can be used by researchers and engineers in the field of IoT to make IoT devices much more convenient in the process of creating that device.

Polychronaki et al. (2023) developed a Proof-of-Concept (PoC) that is based on blockchain technology and demonstrates the access and authorization capabilities of this technology. They investigated whether an authorization system based on blockchain could be designed in such a way to be able to integrate easily with existing IoT environments for easy integration into the future.

According to Ahmed and Khan (2023), the authors considered the Internet of Things ecosystem from a futuristic perspective, and they examined cybersecurity, privacy, and connectivity from the perspective of a future IoT ecosystem. The Internet of Things (IoT) is associated with many attacks, such as attacks that allow for unauthorized access, device spoofing, Man-in-the-Middle attacks, etc. A recent publication of an article by Usmani et al. (2023) argued that there is a need to integrate IoT-enabled sensors with IoT technologies, enabling their deployment and use in both engineering applications and humanitarian contexts. The implementation of robust security measures that ensure the integrity and reliability of IoT systems can make them more reliable and secure by ensuring that they are highly reliable and trustworthy.

According to Zhonghua et al. (2023), IOT engineering is being applied to several humanitarian contexts, including disaster management, healthcare monitoring, environmental monitoring, and infrastructure development, in which IoT is being applied to humanitarian contexts.

According to Thavamani and Nandhini (2023), blockchain security architecture can be categorized into several levels, enabling simplified implementation while bolstering the overall security of the network. In their study, the authors examined the challenges and strategies associated with the security of cloud computing and the Internet of Things. Blockchains, machine learning, cryptography, quantum computing, and machine learning are just a few of the examples we can use.

Several recent articles have described difficulties that have been mentioned in the text of Avik et al. (2023). I have summarized in brief the threats, access control issues, and remedies discussed in this contribution. To create preventative measures for IoT use cases, researchers can analyze some real-life attacks against public blockchain protocols to develop some prevention measures.

As described in the paper of Tyagi (2024), the authors examined the potential synergies that might exist between blockchain technology and artificial intelligence in the context of cybersecurity for the Internet of Things and the Industrial Internet of Things. Khan et al. (2024) demonstrated that machine learning and expert systems can be integrated to develop comprehensive, adaptive

defense systems and that this method is advantageous to the development of these systems.

2.1. Problem statement

In smart cities, the detection and prevention capabilities of traditional security systems are often hindered by complex infrastructure and a lack of real-time information sharing. As a result, there is a growing need for advanced solutions that can proactively identify and respond to potential threats, ensuring the safety and security of residents.

2.2. Objectives of the study

The main aim of this paper is to propose a hybrid smart detection and prevention IoT framework for smart cities using blockchain technology (HDPIoTF) that combines the strengths of both IoT and blockchain technology.

3. Methodology

This study uses a mixed methodology approach, reviewing literature and applying design science to develop a hybrid smart detection and prevention IoT framework for smart cities. The literature review aims to gather and analyze the existing works and highlight the main gaps in the domain, whereas the design science method is used to develop the hybrid smart detection and prevention IoT framework for smart cities using blockchain technology. Fig. 1 displays the adapted methodology.

Step 1: Identifying searching protocols: in this step, the author identifies the searching protocols to govern the behaviors of the searching. These protocols involve: defining the keywords, defining the searching period, defining the searching language, defining the searching questions, and identifying common online databases. According to the study, there are three keywords that are defined in this study which are "Smart cities"; "IoT"; "Detection and Prevention"; and "Blockchain." Accordingly, the search period for this study is defined from 2015-2024, and English is the main language that will be used for this study throughout the entire study period. For this study, the following questions have been prepared:

- What are the existing detection and prevention models/frameworks for IoT smart cities?
- What are the advantages and disadvantages of the existing detection and prevention models/frameworks for IoT smart cities?

Then, five common online databases are defined for this study: Scopus, Web of Science, Springer Link, IEEE Xplore, and Google Scholar.

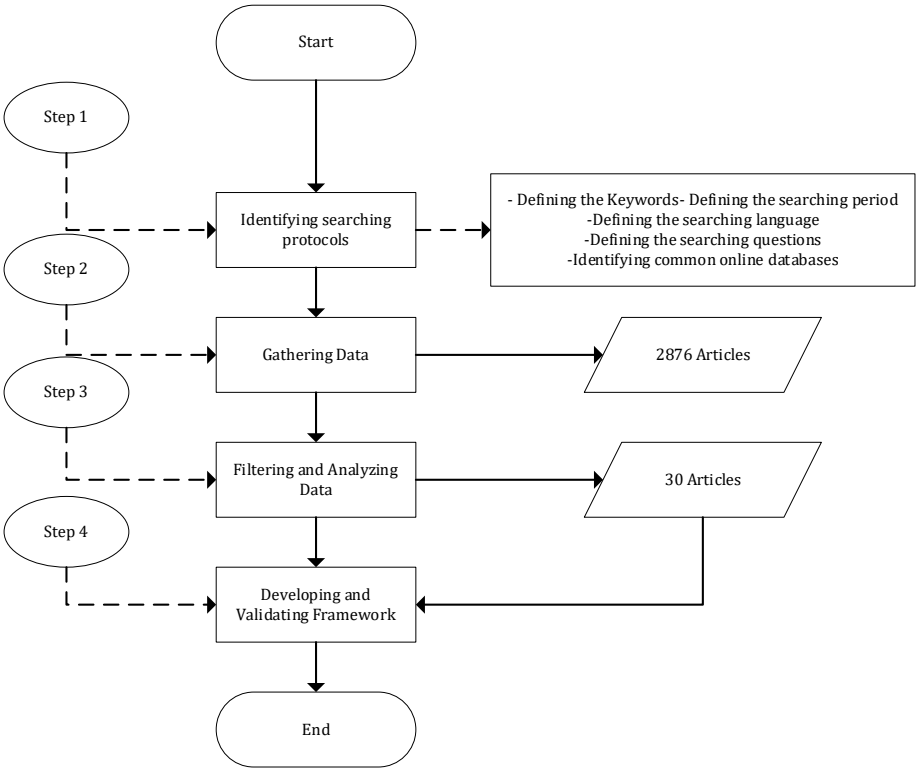

Fig. 1: Adapted research methodology

Step 2: Gathering data: after defining and identifying the searching protocols in Step 1, the data will be gathered in this step. To gather the data, the specified keywords are used to identify relevant articles, books, conference proceedings, and documents. These keywords were selected based on the research questions and objectives defined in Step 1.

In total, 2876 articles have been collected from the five online databases to complete this study. The

number of articles that have been retrieved from Google Scholar is 1800, 948 from Springer Link, 90 from Scopus, eight from Web of Science, and 30 from IEEE Xplore. The next step will be filtering and analyzing the data collected.

Step 3: Filtering and analyzing data: The gathered data will be filtered and analyzed in this step based on inclusion and exclusion criteria. The filtering process involves reviewing each data point and comparing it to the inclusion and exclusion criteria. Data that meets all the criteria is kept, while data that does not meet the criteria is removed. This process. Thus, the inclusion criteria involve:

- The articles should be conference papers, review papers, and article papers.
- The relevant articles are included in.

The exclusion criteria involve:

- Duplicate articles.
- Articles without results.
- Irrelevant articles.

As a result, and following the inclusion and exclusion criteria, 30 articles have been selected to be evaluated for the present study. Those articles are purely focused on the use of smart detection and prevention technologies for smart cities, using the Internet of Things. Following the filtration process, the following paragraphs explain how the 30 articles were analyzed after the filtration process was completed. Table 1 explains the analysis of the 30 articles. It shows the advantages, disadvantages, and output of these articles.

4. Results and discussions

The proposed Hybrid Smart Detection and Prevention IoT framework for Smart Cities Using Blockchain Technology consists of several key components as shown in Fig. 2. The explanation of each component is discussed in Table 2.

In the Hybrid Smart Detection and Prevention IoT Framework, the primary goal is to provide smart detection and prevention capabilities in a connected, intelligent, and automated manner. There are many sources of data that are gathered in smart cities, including surveillance cameras, sensors, and smart devices. Consequently, it has become possible to monitor and analyze urban environments, identify potential risks, and implement prevention measures to make urban environments safer and better. As shown in Table 3, the proposed framework incorporates blockchain technology and offers the following benefits.

The proposed framework can be effectively utilized in various applications of HDPIoTF. Some potential applications are displayed in Table 4.

The Hybrid Smart Detection and Prevention IoT Framework for Smart Cities using Blockchain Technology represents a significant advancement in smart city infrastructure. This framework leverages both IoT and blockchain technologies to create a robust, scalable, and cost-effective solution for urban management and security. Cost-effectiveness is another major advantage of this framework. By utilizing blockchain, the need for expensive centralized servers and data storage solutions is reduced. The distributed ledger technology allows for secure and transparent data transactions without the need for intermediaries, which significantly lowers operations. The ease of implementation is facilitated by the modular design of the framework. The integration of IoT devices with blockchain technology is streamlined through standardized protocols and interfaces, making it easier to deploy and manage. The framework's architecture allows for plug-and-play functionality, enabling city planners and administrators to add or remove devices and services as needed without extensive reconfiguration.

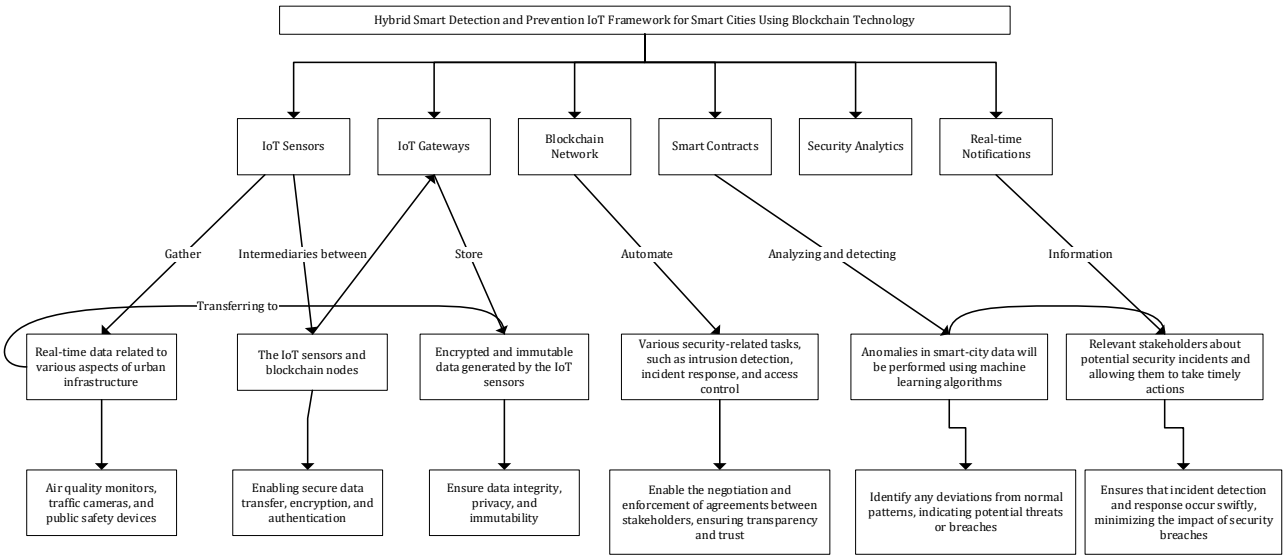

Fig. 2: Hybrid smart detection and prevention IoT framework for smart cities using blockchain technology

Table 1: Existing IoT security models and framework solutions for smart cities

Reference	Benefits	Drawbacks	Methodology or mechanisms	Output
Martins (2018)	Securing communication between small devices and platforms is possible.	Lacks implementation	Survey and interview	Proposed establishing a "mini laboratory," consisting of a wide range of minor tools with a variety of interaction capabilities
Fayad et al. (2018)	Optimize IoT security through adaptive authentication and authorization.	Data encryption, data protection, and security, as well as gateway access to secure information, are among the concerns raised by the blockchain.	Design science method	Proposed adaptive authentication and authorization method based on blockchain technology
Prathibha and Fatima (2018)	Determine which security risks are associated with the Internet of Things using current and future security techniques based on Internet of Things concepts. Additionally, a framework for IoT authentication was proposed.	Lack of implementation.	Design science method	Presented a framework for the verification of IoT schemes, such as home mechanization systems.
Rashid and Pajooh (2019)	It is possible to optimize the network lifetime with the assistance of genetic algorithms and particle swarm optimization by clustering the network into K unknown clusters.	The ability to optimize network lifetime in this manner is not impressive, even if it seems to work.	The use of genetic algorithms for optimization	Proposed strategy for self-clustering IoT networks
Ware (2019)	Evaluated research has been supervised on protection challenges and confidentiality challenges in smart cities.	They failed to provide any analysis of the research that has been carried out on these topics.	Design science method	Propose security mechanisms for smart city IoT infrastructures and authentication mechanisms for smart cities.
Anawar et al. (2019)	The contribution of this study is to determine the impact of future technological adoption on potentially impacted areas in terms of expected and unexpected geopolitical implications. A third contribution is to make recommendations to mitigate geopolitical risks	Lack of implementations	Design science method	Prospects and implications of IoT technology for hyperstability
Muzammal and Murugesan (2020)	Explored the security concerns and issues associated with IoT. Provided an overview of centralized as well as decentralized IoT security platforms based on authentication and authorization in terms of the level of security. Discussed how blockchain technology can be used to provide security for IoT devices.	Ineffectiveness and inefficiency due to lack of scalability	Blockchain technology	Discussed how blockchain technology can be used to provide security for IoT devices
Mohammad and Abdulqader (2020)	Investigated the essential cyber security requirements for smart cities following the research that has been carried out previously in this field.	The implementation and maintenance of cybersecurity measures in smart cities require significant investment and resources.	Systematic research design	Exploring cybersecurity measures in smart cities is crucial for ensuring the security and privacy of citizens
Chaabouni (2020)	It suggested that the Internet of Things network be separated into several layers of reorganized organizations to solve some of the issues with the Internet of Things, in addition to implementing blockchain technology to solve some of the problems.	The IoT network would need to be divided into multiple layers of decentralized systems to solve the problems associated with its implementation. To solve the implementation challenges associated with blockchain technology, the IoT network would have to be broken into multiple layers.	Design science method	Developed a multilayer protection network model to be used for IoT systems.
Mudawi (2020)	Protecting IoT devices in smart homes requires several complementary engines working together. The detection of anomalies in home network traffic is the basis for IDS/IPS and packets are identified, alerted, and/or blocked if any anomalous activity is detected.	Lack of implementation and testing.	Design science method	Proposed a framework for the protection of smart homes
Khalil et al. (2022b)	The paper presents a breakdown of blockchain-based authentication mechanisms that enable decentralized architectures.	The limitations of scalability, the use of energy, the privacy concerns, the interoperability challenges, and the governance and regulation concerns should all be considered to implementing blockchain technology in smart cities	Blockchain technology and IoT-enabled smart devices.	Presented updated information on authentication mechanisms that support decentralized architectures.
Asif et al. (2022)	Providing heterogeneous smart city technologies with a user-friendly interface is the goal of a hybrid application	Blockchains are difficult to implement and deploy in government institutions because they are untrustworthy and uncontrollable.	Blockchain technology	An efficient and reliable method for managing trust and authentication was presented.
Mohammad et	By using sender time stamps, IoT devices can authenticate and verify their	The real implementation is lacking.	Internet of Things	Presented and implemented a new

al. (2022)	identities more efficiently, allowing them to reduce their local identity verification requirements. Testing was performed against different types of attacks in comparison with previous related frameworks. A wide range of attacks can be prevented by the proposed framework for IoT networks. Simulations, checks of validity, and calculations of payload times were performed using Windows applications.			enhanced IoT security framework that protects IoT protocols from attacks such as man-in-the-middle, reply, and brute force attacks, as well as other threats.
Bhardwaj et al. (2022)	Determine privacy risks in IIoT devices	Ecosystems are insecure because of both risks.	Internet of Things, Authentication, Key management	Developed and analyzed a novel framework for analyzing industrial Internet of Things (IIoT) threats.
Fei (2022)	Created an IoT gateway that is safe, efficient, and secure and can be used by IoT researchers and engineers as they work on IoT devices as part of their research.	Due to the large number of packet characteristics needed to analyze, it costs a lot of money to run and detect only a limited number of attacks.	Raspberry	Developed an IoT gateway
Polychronaki et al. (2023)	Investigated whether an authorization system based on blockchain could be designed in such a way to be able to integrate easily with existing IoT environments for easy integration into the future.	Lack of implementation in the real world.	IoT, and Blockchain technology	Developed a Proof-of-Concept (PoC)
Ahmed and Khan (2023)	Improves device and network resilience, protecting them from malicious attacks. It enables the implementation of robust access controls and encryption protocols, safeguarding sensitive information	implementing security in IoT systems can be complex and costly. It requires continuous monitoring, updates, and collaboration between stakeholders, adding overhead to system management	Systematic research design	In the era of Internet of Things, security, privacy, and connectivity are of utmost importance
Usmani et al. (2023)	The potential for real-time monitoring and evaluation of humanitarian operations. With the integration of IoT technologies, data can be collected and analyzed more efficiently, enabling organizations to make data-driven decisions and improve their interventions.	IoT technologies require robust security measures to prevent unauthorized access and data breaches. Additionally, the reliance on IoT infrastructure can make systems vulnerable to disruptions or failures, potentially impacting the delivery of critical services.	Systematic research design	Internet of Things technologies and sensors integrated with security features
Zhonghua et al. (2023)	Provides decentralized authentication to reduce the risk of single points of failure. Attribute-based access control (ABAC) restricts access to sensitive resources.	One of the major drawbacks is the complexity of implementing and managing smart contracts. Additionally, blockchain transaction fees can be high, which can impact scalability. Moreover, edge computing infrastructure can be vulnerable to physical attacks	Blockchain technology	Presented IoT engineering applications in humanitarian contexts
Thavamani and Nandhini (2023)	Increased efficiency and scalability, reduced costs, and improved collaboration.	One disadvantage is that cloud-based systems and IoT networks are susceptible to data breaches and cyber-attacks. This can result in the loss of sensitive information, identity theft, and financial losses.	Blockchain, machine learning, cryptography, and quantum computing	Proposed blockchain security architecture with multi-levels to simplify implementation while bolstering network security.
Alghamdi et al. (2023)	Enhance security while simplifying implementation for the global layers. In this model, clustering provides local-global architecture, with cluster heads responsible for individual authentication and authorization. By implementing a local private blockchain, cluster heads, and relevant bases can communicate seamlessly	Lack of implementation in the real world.	Blockchain technology	Proposed a new blockchain model based on local and global layers.

Table 2: Explanation of HDPIoTF

Component	Explanation
IoT sensors	Gather timely data from various sources, enhancing decision-making processes
IoT gateways	Act as hubs that aggregate data from sensors and devices, ensuring secure communication with the cloud
Blockchain network	Establish a secure framework for data integrity and confidentiality, enabling decentralized management
Smart contracts	Automate processes and enforce agreements, enhancing security and transparency in transactions
Security analytics	Use machine learning to detect anomalies and prevent security threats through real-time monitoring
Real-time notifications	Facilitate immediate alerts to stakeholders, ensuring responsiveness to security incidents

Table 3: Benefits of HDPIoTF

Benefit	Explanation
Data security and privacy	Blockchain technology provides a secure and tamper-proof data storage and transmission environment, making it difficult for unauthorized individuals to access or tamper with sensitive information
Transparency and accountability	Blockchain integration allows transparent data management and audit trails, ensuring information can be shared among authorized parties without compromising privacy while reinforcing accountability in decision-making processes
Real-time data sharing	Blockchain enables real-time data sharing and collaboration. Data from multiple sensors can be aggregated and analyzed, enabling real-time detection of anomalies and potential threats
Ethical data use	Blockchain technology promotes ethical data use by enabling data ownership and control, allowing individuals to exercise their rights over their data, and ensuring it is used responsibly and ethically

Table 4: Potential applications that can be utilized by the developed HDPIoTF

Potential applications	Explanations
City-wide security	The framework can be utilized to monitor and secure entire cities, detecting potential threats and ensuring real-time alerts can be triggered, enabling prompt responses
Smart traffic management	Traffic patterns can be analyzed to identify bottlenecks and congestion points, enhancing efficient traffic management and optimization

Furthermore, the use of smart contracts on the blockchain automates many processes, reducing the complexity and time required for implementation. This plug-and-play and automated approach simplifies the deployment process, making it accessible even for cities with limited technical expertise. Also, the Hybrid Smart Detection and Prevention IoT Framework provides deeper insights into urban management by combining real-time data from IoT devices with the immutable and transparent nature of blockchain.

5. Validation

The validation of the proposed HDPIoTF is archived in this section from two perspectives: comparing with other models (Sargent, 2015; Alfadli et al., 2021), and implementation in the real scenario (Ali et al., 2022). Comparison with other models is used to check the completeness and generalization of the proposed HDPIoTF. The second step in implementing the developed HDPIoTF for Smart Cities Using Blockchain Technology is to evaluate its applicability in real-world scenarios.

Therefore, Table 5 describes the validation of the developed HDPIoTF with existing detection and prevention smart cities models and frameworks. The developed HDPIoTF is comprehensive and can cover the existing detection and prevention techniques used to prevent and detect cybercrime in smart cities. The HDPIoTF has been successfully tested against existing models, and the results are promising. The HDPIoTF can be used to further enhance smart cities' cybersecurity. Additionally, the HDPIoTF can be applied to a wide range of smart cities, regardless of their size or complexity.

Table 5: Comparing the developed HDPIoTF and the existing models and frameworks

	Existing works																				
Proposed HDPIoTF	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
IoT sensors	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	⊗	⊗	⊗
IoT gateways	⊗	✓	⊗	⊗	✓	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	⊗	⊗	⊗	⊗	⊗	⊗
Blockchain network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart contracts	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	⊗	⊗
Security analytics	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	⊗
Real-time notifications	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗

1: Martins (2018); 2: Fayad et al. (2018); 3: Prathibha and Fatima (2018); 4: Rashid and Pajooh (2019); 5: Ware (2019); 6: Anawar et al. (2019); 7: Muzammal and Murugesan (2020); 8: Mohammad and Abdulqader (2020); 9: Chaabouni (2020); 10: Mudawi (2020); 11: Khalil et al. (2022b); 12: Asif et al. (2022); 13: Mohammad et al. (2022); 14: Bhardwaj et al. (2022); 15: Fei (2022); 16: Polychronaki et al. (2023); 17: Ahmed and Khan (2023); 18: Usmani et al. (2023); 19: Zhonghua et al. (2023); 20: Thavamani and Nandhini (2023); 21: Alghamdi et al. (2023)

In the second validation technique, the HDPIoTF is implemented and verified using the following real-life scenarios: Scenario 1: Smart City Traffic Control System: City A has implemented a smart traffic control system that uses IoT sensors to detect traffic congestion in real time. The traffic control system is equipped with surveillance cameras, which capture and analyze traffic data. The captured data is stored

and processed in the cloud, where machine learning algorithms analyze patterns and provide valuable insights to the city's traffic management department. However, City A recognizes the need for a more robust and secure system. HDPIoTF can provide the necessary security measures.

6. Conclusion

In the era of smart cities, there are tremendous opportunities to enhance cybersecurity and public safety by enhancing the Internet of Things (IoT) and the Internet of Things (IoT). As smart city technology continues to grow and complexity increases, securing these cities from cyber threats becomes a more challenging task, due to the rapid growth and complexity of these technologies. As a solution to this issue, we proposed a hybrid smart detection and prevention IoT framework (HDPIoTF) based on blockchain technology for smart cities. Our goal is to integrate IoT and blockchain technology to construct a smart city system that combines IoT and blockchain technology effectively and robustly. There are six stages included in the framework developed: sensor development, gateway development, IoT gateway development, blockchain development, smart contracts development, security analytics, and real-time notifications within the context of the real-time monitoring system. For this article, design science has been used as the method of analysis. In this project, blockchain technologies and the Internet of Things are used to monitor real-time data, to provide enhanced security, automated responses, interoperability, and enhanced security through real-time monitoring and enhanced security. Moreover, it ensures the safety and security of critical infrastructure, thereby improving the quality of life and well-being of citizens in the process. The future work of this study is to validate the developed model in real scenarios.

Compliance with ethical standards

Conflict of interest

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

References

Adel A and Alani NH (2024). Human-centric collaboration and Industry 5.0 framework in smart cities and communities: Fostering sustainable development goals 3, 4, 9, and 11 in Society 5.0. Smart Cities, 7(4): 1723–1775. https://doi.org/10.3390/smartcities7040068

Ahmed S and Khan M (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. AI, IoT and the Fourth Industrial Revolution Review, 13(9): 1-17.

Alfadli IM, Ghabban FM, Ameerbakhsh O, AbuAli AN, Al-Dhaqm A, and Al-Khasawneh MA (2021). CIPM: Common identification process model for database forensics field. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 72-77. https://doi.org/10.1109/ICSCEE50312.2021.9498014

Alghamdi S, Albeshri A, and Alhusayni A (2023). Enabling a secure IoT environment using a blockchain-based local-global consensus manager. Electronics, 12(17): 3721. https://doi.org/10.3390/electronics12173721

Ali A, Razak SA, Othman SH, Marie RR, Al-Dhaqm A, and Nasser M (2021). Validating mobile forensic metamodel using tracing method. In the International Conference of Reliable Information and Communication Technology, Springer International Publishing, Cham, Switzerland, 127: 473-482. https://doi.org/10.1007/978-3-030-98741-1_39

Anawar S, Zakaria NA, Masu'd MZ, Muslim Z, Harum N, and Ahmad R (2019). IoT technological development: Prospect and implication for cyberstability. International Journal of Advanced Computer Science and Applications, 10(2): 428-437. https://doi.org/10.14569/IJACSA.2019.0100256

Asif M, Aziz Z, Bin Ahmad M, Khalid A, Waris HA, and Gilani A (2022). Blockchain-based authentication and trust management mechanism for smart cities. Sensors, 22(7): 2604. https://doi.org/10.3390/s22072604 **PMid:35408219 PMCid:PMC9003294**

Avik SC, Biswas S, Ahad MAR, Latif Z, Alghamdi A, Abosaq H, and Bairagi AK (2023). Challenges in blockchain as a solution for IoT ecosystem threats and access control: A survey. Arxiv Preprint Arxiv:2311.15290. https://doi.org/10.48550/arXiv.2311.15290

Bhardwaj A, Kaushik K, Bharany S, Rehman AU, Hu YC, Eldin ET, and Ghamry NA (2022). IIoT: Traffic data flow analysis and modeling experiment for smart IoT devices. Sustainability, 14(21): 14645. https://doi.org/10.3390/su142114645

Buyannemekh B and Cook ME (2023). Navigating information technology challenges and priorities: Expanding responsibilities, growing roles, and evolving contexts for city leaders. In the Proceedings of the 24th Annual International Conference on Digital Government Research, ACM, Gdańsk, Poland: 478-485. https://doi.org/10.1145/3598469.3598523

Chaabouni N (2020). Intrusion detection and prevention for IoT systems using machine learning. Ph.D. Dissertation, Université de Bordeaux, Bordeaux, France.

Fayad A, Hammi B, and Khatoun R (2018). An adaptive authentication and authorization scheme for IoT's gateways: A blockchain based approach. In the 3rd International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE, Shanghai, China: 1-7. https://doi.org/10.1109/SSIC.2018.8556668

Fei W (2022). Raspberry house: An intrusion detection and prevention system for Internet of Things (IoT). M.Sc. Thesis, Dalhousie University, Halifax, Canada.

Khalil U, Malik OA, and Hussain S (2022a). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access, 10: 76805-76823. https://doi.org/10.1109/ACCESS.2022.3189998

Khalil U, Malik OA, Uddin M, and Chen CL (2022b). A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions. Sensors, 22(14): 5168. https://doi.org/10.3390/s22145168 **PMid:35890848 PMCid:PMC9322843**

Khan IU, Ouaissa M, Ouaissa M, Abou El Houda Z, and Ijaz MF (2024). Cyber security for next-generation computing technologies. CRC Press, Boca Raton, USA.

Martins RMS (2018). Secure and high-performance framework for smart cities based on IoT. M.Sc. Thesis, Universidade do Minho, Braga, Portugal.

Mohammad A, Al-Refai H, and Alawneh AA (2022). User authentication and authorization framework in IoT protocols. Computers, 11(10): 147. https://doi.org/10.3390/computers11100147

Mohammad RMA and Abdulqader MM (2020). Exploring cyber security measures in smart cities. In the 21st International Arab Conference on Information Technology, IEEE, Giza, Egypt: 1-7. https://doi.org/10.1109/ACIT50332.2020.9300050

Mudawi T (2020). IoT-HASS: A framework for protecting smart home environment. Ph.D. Dissertation, Dakota State University, Madison, USA.

Muzammal SM and Murugesan RK (2019). A study on secured authentication and authorization in Internet of Things: Potential of blockchain technology. In the International Conference on Advances in Cyber Security, Springer Singapore, Penang, Malaysia: 18-32. https://doi.org/10.1007/978-981-15-2693-0_2

Polychronaki M, Kogias DG, Leligkou HC, and Karkazis PA (2023). Blockchain technology for access and authorization management in the Internet of Things. Electronics, 12(22): 4606. https://doi.org/10.3390/electronics12224606

Prathibha L and Fatima K (2018). Exploring security and authentication issues in Internet of Things. In the 2nd International Conference on Intelligent Computing and Control Systems, IEEE, Madurai, India: 673-678. https://doi.org/10.1109/ICCONS.2018.8663111

Rao PM and Deebak BD (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(8): 10517-10553. https://doi.org/10.1007/s12652-022-03707-1

Rashid MA and Pajooh HH (2019). A security framework for IoT authentication and authorization based on blockchain technology. In the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, Rotorua, New Zealand: 264-271. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00043

Sargent RG (2015). Model verification and validation. In: Loper ML (Ed.), Modeling and simulation in the systems engineering life cycle: Core concepts and accompanying lectures: 57-65. Springer, London, UK. https://doi.org/10.1007/978-1-4471-5634-5_6

Thavamani S and Nandhini C (2023). Major security issues and data protection in cloud computing and IoT. In: Sajid M, Sagar AK, Singh J, Khalaf OI, and Prasad M (Eds.), Intelligent techniques for cyber-physical systems: 317-336. CRC Press, Boca Raton, USA. https://doi.org/10.1201/9781003438588-18

Tyagi AK (2024). Blockchain and artificial intelligence for cyber security in the era of Internet of Things and Industrial Internet of Things applications. In: Biradar RC, Tabassum N, Hegde N, and Lazarescu M (Eds.), AI and blockchain applications in industrial robotics: 171-199. IGI Global, Hershey, USA. https://doi.org/10.4018/979-8-3693-0659-8.ch007

Usmani UA, Happonen A, and Watada J (2023). Secure integration of IoT-enabled sensors and technologies: Engineering applications for humanitarian impact. In the 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, IEEE, Istanbul, Turkiye: 1-10. https://doi.org/10.1109/HORA58378.2023.10156740

Ware JC (2019). Secure authentication mechanisms for smart city IoT infrastructure. M.Sc. Thesis, Utica College, Utica, USA.

Zhonghua C, Goyal SB, and Rajawat AS (2024). Smart contracts attribute-based access control model for security and privacy of IoT system using blockchain and edge computing. The Journal of Supercomputing, 80(2): 1396-1425. https://doi.org/10.1007/s11227-023-05517-4