IoT Security Model for Smart Cities based on a Metamodeling Approach

Daifallah Zaid Alotaibe
Software Engineering Department, College of Computer Science and Engineering, University of Hafr Al-Batin, Saudi Arabia
dzalotaibe@uhb.edu.sa (corresponding author)

Received: 23 February 2024 | Revised: 8 March 2024 and 21 March 2024 | Accepted: 28 March 2024

ABSTRACT

Security solutions for the Internet of Things (IoT) in smart cities are complex and require a comprehensive approach to success. Several models and frameworks have been developed focusing on IoT security. Some deal with access controls and security and some with authentication and authorization in various forms. Literature still lacks a comprehensive IoT security model for smart cities, which can support the implementation of IoT. Accordingly, this study has set two objectives: to explore the present studies in IoT security for smart cities and to develop an IoT security model for smart cities based on the metamodeling approach. According to the findings of the study, the existing IoT security models for smart cities consider seven security aspects: authentication and authorization, device management, intrusion detection and prevention, device integrity, secure communication, secure data storage, and response to security incidents. The model developed in this study, called IoT Security Metamodel (IoTSM), combines these aspects. IoTSM captures the main qualities of IoT security practices in smart cities through domain security processes.

Keywords-IoT security; smart cities; metamodel; metamodeling

I. INTRODUCTION

During the recent years, with the rapid development of computer science and information and communication technologies, the vision of building smart cities has become closer to reality [1, 2] This process has been expedited with developments, such as the Internet of Things (IoT), cloud computing, and social networking [3-5]. Securing smart cities is a complicated task, which requires a comprehensive approach to IoT security solutions. Smart cities can minimize the risks associated with interconnected devices and improve their resilience to cyber threats by implementing robust authentication and access controls, encrypting data, regularly patching, and updating, implementing intrusion detection and prevention systems, segmenting networks, and establishing secure communication channels. It is crucial to all stakeholders, including city administrators, technology providers, and residents, to collaborate and prioritize the security of smart cities to ensure the well-being of people and the overall functioning of urban infrastructure. Several researchers have attempted to solve IoT security issues of smart cities from different perspectives. However, the already proposed models tend to focus on specific issues, for example, some have focused on authentication and authorization, some on integrity, and some on secure channels. As a result, IoT security for smart cities is a heterogeneous, ambiguous, and complex domain and lacks a comprehensive method to unify all the IoT security models into one harmonized framework that organizes the IoT security domain for smart cities. Therefore, this study explores IoT security solution models and frameworks for smart cities and develops a new model, called IoT Security Metamodel (IoTSM), based on a metamodeling approach to solve security issues of smart cities. The metamodeling approach is used to integrate and define models [6, 7]. Metamodeling can be employed for many purposes, including normalization. The term metamodeling refers to the identification and association of general practices in each problem domain. According to [8], it is utilized to solve complex problems relating to interoperability and heterogeneity in the domain. For that reason, metamodels should be well structured and rigorously defined. The novelty of this study lies in its comprehensive examination of the main issues and challenges in IoT security for smart cities and the development of IoTSM, which can structure and organize the IoT security practices field. By accomplishing these objectives, this study aims to contribute to the advancement of IoT security in smart cities.

II. RELATED WORKS

Research and synthesis of existing knowledge on a particular topic can be accomplished by conducting a literature review, which is an important step in the research process. In order to achieve a comprehensive understanding of a topic, it is crucial to carry out a systematic analysis and synthesis of the existing literature. In order to obtain relevant information, identify gaps, and formulate new research questions or hypotheses, we rely on this analytical method of collecting information. The adapted methodology consists of four steps:

1. **Recognition step**: Six search engines were considered in this step, namely Google Scholar, IEEE Explore, Science Direct, Scopus, Springer Link, and Web of Science (WoS), as sources for gathering models of IoT security. Papers in English published from 2010 to 2024 about IoT security for smart cities were collected. The search process used "IoT security" and "Smart cities" as keywords. A total of 309 articles were gathered.
2. **Filtering Step**: In this step, the gathered articles were filtered based on the title, abstract, and conclusion. All 309 articles were filtered, among which 210 articles were omitted because of repetition.
3. **Elimination Step**: In this step, some of the articles were eliminated based on numerous conditions. For example, 181 articles were eliminated for reasons, such as irrelevance and limited findings.
4. **Inclusion Step**: In this step, 29 articles were contained and considered as they concentrated solely on smart cities and IoT security as shown in Table I.

Several models have been proposed in the literature for the IoT security of smart cities. For example, authors in [9] suggested creating a mini laboratory comprising a wide variety of small devices with numerous interaction abilities. These rooted devices are equipped with several sensors that can obtain data, such as humidity, temperature, and light from their environment. Numerous small devices/platforms were discussed regarding secure communication between them. In [10], the authors proposed an adaptive blockchain-based authentication and authorization method for IoT. Their approach was implemented using Java. The widespread offered evaluation reveals their scheme's ability to meet different requirements and ensure a low cost. Authors in [11] evaluated existing IoT-based security methods and provided some directions for future research in this innovative field. They explored local security issues relating to IoT. Furthermore, as part of smart IoT systems, like Home Automation Systems, the researchers also introduced an IoT-based authentication framework.

Authors in [12] examined the technologies adopted in smart cities, the cyber threats they pose to residents, businesses, and visitors, and the ethical implications these technologies may have. Following a layered defense approach, the former reduced the attack surface and isolated business impacts. They implemented threat prevention for improved visibility and control and set up software-defined perimeters and networks segmented with a central security policy platform that enforced policies and responded in real-time to cyberattacks. Authors in [13] proposed a multilayer security network model for IoT networks. In the recommended model, the IoT network is divided into multiple layers of decentralized systems to solve the problems mixed with the actual implementation of blockchain technology. Specifically, authors in [14] examined peer-to-peer, gateway-based, and biometric-based authentication mechanisms for IoT infrastructure. Furthermore, they evaluated the research on challenges relating to security and privacy in smart cities. Authors in [15] provided a roadmap that outlines future technology security needs and concerns, as well as the role that IoT can play in addressing those needs. Authors in [16] reviewed centralized and decentralized IoT security solutions with regard to authentication and authorization. They also discussed the potential of blockchain technology regarding security. Authors in [17] examined the essential cyber security requirements in smart cities based on previous research. Moreover, several other security demands were introduced aiming to fill knowledge gaps. Authors in [18] stated that a system based on machine learning would be effective in protecting IoT systems from intrusions and detecting them early on when they occur. The proposed framework for securing smart homes in [19] consists of three complementary engines for protecting IoT devices in smart homes. Using anomaly-based detection, the suggested Intrusion Detection Systems/ Intrusion Prevention System (IDS/IPS) monitors all traffic in the home network and detects, alerts, and/or blocks packets that are spotted based on anomaly detection. Authors in [20] proposed a machine-readable, standardized framework for sharing cyber threat intelligence. Deploying blockchain as an underlying technology for collaboration and data exchange, they demonstrated the effectiveness and security of securing home networks and the shared IoT devices with a series of experiments.

According to [21], authentication and authorization for constrained environments and OSCAR-based object security models could be combined to create a framework-based authorization blockchain that could be used for any application. Authors in [22] developed an enhanced authentication and authorization framework for IoT. An identity verification mechanism was developed on the IoT-device side based on time stamps, which reduced the need for local identity verification methods by implementing token authentication with identity verification capabilities. Authors in [23] found that security and privacy are primarily concerned with authentication mechanisms and key agreements that serve as a basis for evaluations of multi-criteria authentication techniques, such as two-factor, three-factor, and multiple-factor authentication. As opposed to analyzing individual nodes of IoT ecosystems, authors in [24] examined the entire ecosystem's vulnerabilities and proposed a unique threat model framework for analyzing attacks on IoT application environments. A physical exchange between IoT devices was explored at the application level based on the identification of sensitive data flows. Authentication mechanisms were categorized into centralized and distributed architectures in [25] and IoT-enabled devices were discussed for their security issues. The authors examined and analyzed the findings regarding computational costs, communication overheads, and robustness of the proposed literature schemes. Authors in [26] proposed Raspberry House, a security gateway that monitors and prevents IoT intrusions.

Denial-of-Service attack on IoT devices is one of the most common major threats a network might face. This attack affects the data link, network, transport, and system layers. In [27], two identity and authentication solutions were presented as a proof-of-concept based on solidity smart contracts. Blockchain is effective for decentralized Identity and Access Management (IAM), and manufacturers can integrate it seamlessly into existing IoT systems without redeveloping them. Blockchains are designed to simplify implementation while increasing security [28], in which, as a result of clustering, authentication and authorization were handled locally by cluster heads. Authors in [29] examined the IoT ecosystem from cybersecurity, privacy, and connectivity perspectives.

Several attacks, including unauthorized access, device spoofing, and Man-in-the-Middle attacks, are intrinsic to IoT environments. Engineering applications and humanitarian context were explored in [30], integrating IoT-enabled sensors and technologies. The authors discussed ways to ensure the reliability and integrity of IoT systems by implementing robust security measures. Authors in [31] presented IoT engineering applications in the humanitarian context, entailing disaster management, healthcare monitoring, environmental monitoring, and infrastructure development. Multi-level blockchain security architectures were proposed in [32, 33] to simplify implementation while bolstering network security. A more recent study [34], examined the challenges and strategies related to cloud computing and IoT security. Using blockchain, machine learning, cryptography, and quantum computing as examples, authors in [35] reviewed potential solutions for securing IoT by comparative analysis of the related papers. Then, they classified the relevant solutions based on their stated requirements for security. Authors in [36], in a variety of approaches, involving blockchain-based solutions, summarized difficulties outlined in numerous recent articles. They summarized threats, access control issues, and remedies.

TABLE I. EXISTING IOT SECURITY MODELS

Year	Ref.	Focal points
2018	[9]	Creation of a mini laboratory comprising a wide variety of small devices with numerous interaction abilities
2018	[10]	Adaptive blockchain-based authentication and authorization method for IoT
2018	[11]	Evaluating the existing IoT-based security methods and future research, exploring local security problems connected to IoT; and introducing an IoT-based authentication framework, as part of smart IoT systems.
2018	[12]	The technologies driving smart cities, the cyber threats they pose to residents, businesses, and visitors, and the ethical implications these technologies may have are examined. A layered defense approach is used to reduce the attack surface and isolated business impacts.
2019	[13]	Multi-layer security network model for IoT networks.
2019	[14]	Examining peer-to-peer, gateway-based, and biometric-based authentication mechanisms for IoT infrastructure.
2019	[15]	Povides a roadmap that outlines the needs and concerns of the future technology security, and discusses the role that IoT can play in addressing those needs.
2020	[16]	Authentication and authorization solutions for IoT, both centralized and decentralized, are reviewed providing information on IoT security.The possibilities of blockchain are discussed.
2020	[17]	A framework for authentication and authorization in IoT devices is proposed and incorporateds into a standard security framework for IoT devices. A new sender verification mechanism based on time stamps was developed on the device side of the IoT, allowing for token authentication with identity verification capabilities and reducing the need for local identity verification methods at the device side.
2020	[18]	The practicality of developing a system based on machine learning to protect IoT systems from intrusions and detect them early on when they occur was investigated.
2020	[19]	A framework for securing smart homes was proposed, consisting of three complementary engines for protecting IoT devices in smart homes, and using anomaly-based detection, where the IDS/IPS monitors all traffic in the home network and detects, alerts, and/or blocks packets based on anomaly detection.
2021	[20]	A machine-readable, standardized framework for sharing cyber threat intelligence and using blockchain as an underlying technology for collaboration and data exchange is proposed in order to demonstrate the effectiveness and security of securing home networks and common IoT devices.
2022	[61]	Review of authentication schemes for IoT for smart cities.
2022	[21]	Proposing a framework-based authorization blockchain based on authentication and authorization for constrained environments and an OSCAR-based object security model.
2022	[22]	Proposing and implementing an enhanced IoT security framework for authentication and authorization.
2022	[23]	Multi-criteria authentication techniques such as two-factor, three-factor, and multifactor authentication are assessed.
2022	[24]	The vulnerabilities of Industrial IoT ecosystems as individual nodes are examined.
2022	[26]	Raspberry House, a security gateway for monitoring and preventing IoT intrusion is proposed, where IoT security gateway targets Denial of Service attacks on IoT devices, at the level of the data link, network, and transport layers, as well as the system security layer.
2023	[27]	A proof-of-concept design is demonstrated and a solidity smart contract-based IAM solution is implemented, and the challenges associated with integrating blockchain in existing IoT systems are identified, which prevents manufacturers from redesigning or redeveloping IoT systems.
2023	[28]	A blockchain model that simplifies implementation while enhancing security, handling authentication and authorization locally by cluster heads, and leveraging the concept of clustering is proposed.
2023	[29]	The IoT ecosystem is examined in depth, focusing primarily on cybersecurity, privacy, and connectivity.
2023	[30]	Ways that IoT-enabled technologies and sensors can be integrated securely into humanitarian applications are investigated.
2023	[31]	Managing access control in IoT environments in a decentralized, fine-grained, and dynamic way to help distributed systems reach consensus faster.
2023	[32]	A multi-level blockchain security architecture to simplify the implementation while strengthening network security is deployed.
2023	[34]	Major difficulties with cloud computing, IoT, and Cloud-IoT security and strategies are discussed.
2023	[35]	Emerging and traditional approaches to IoT security are discussed, including blockchain, machine learning, cryptography, and quantum computing.
2023	[36]	Several articles are reviewed and various attacks and security challenges are discussed, including blockchain-based approaches.
2024	[37]	The potential synergies between blockchain and artificial intelligence in cyber security for IoT and Industrial IoT are discussed.
2024	[38]	The combination of expert systems and machine learning with the aim of developing a comprehensive and adaptive defense is examined.

Researchers can take preventative measures for IoT use cases through exploring some real-life attacks against public blockchain protocols. Authors in [38] reviewed the potential synergies between blockchain and artificial intelligence in the context of cybersecurity for IoT and the Industrial IoT. Authors in [38] demonstrated the benefits of integrating machine learning with expert systems for the development of comprehensive and adaptive defense systems. Multiple investigation works have been proposed in the literature to detect smart city crimes [39-59] to assess the risk of cybercrimes, data breaches, and other digital malevolent incidents.

III. METHODOLOGY

This study followed the metamodeling approach to develop an IoT security metamodel for smart cities. The metamodeling approach is used for integrating and defining models across various domains [6]. Some common practices can be identified and shared among these different views. Thanks to its flexibility, metamodeling can be applied in a few different domains, especially where consistency is required [41]. It involves detecting the general practices and their relationships that exist in each problem area. The metamodeling approach solves difficulties in the field, promotes interoperability, and removes divergences [8]. The metamodeling utilized in this study consists of four steps, as displayed in Figure 1.

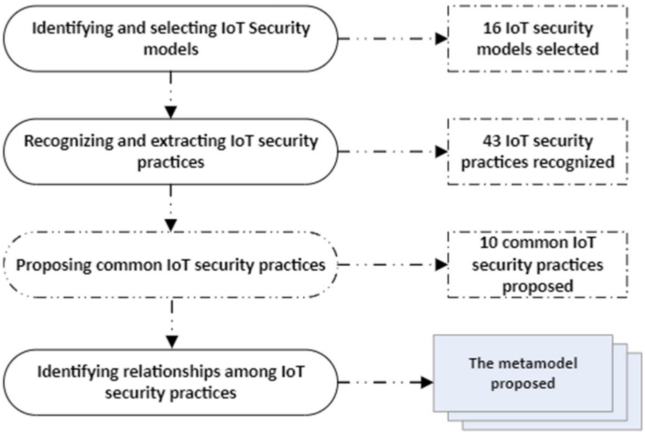
Identifying and selecting IoT Security models
16 IoT security models selected
Recognizing and extracting IoT security practices
43 IoT security practices recognized
Proposing common IoT security practices
10 common IoT security practices proposed
Identifying relationships among IoT security practices
The metamodel proposed

Fig. 1. Methodology used in this research.

1. **Identifying and selecting IoT security models*:*** Several IoT security models for smart cities were discussed in Section 2. Model selection for this study was based on the coverage factors identified in [62]. There is a need for a wide coverage of IoT security perspectives that are broadly applicable in order to achieve the aim of proposing a common IoT security practice. A model can be said to have a high coverage value when it can cover four or more IoT security perspectives. Therefore, and based on the above criteria, 16 IoT security models were found to cover four or more IoT security perspectives. These models were selected for the development of this study's metamodel (see Table II). The next step discusses the way the IoT security practices were recognized and extracted from the selected models.
2. **Recognizing and extracting IoT security practices**: In this step, the IoT security practices for smart cities were extracted from the 16 selected models based on criteria adopted from [63, 64]:
   a. Titles, abstracts, related works, and conclusions were excluded. The IoT security practices for smart cities were extracted from the diagram or the main textual model.
   b. IoT security practices for smart cities had to have a definition, activity, or task to recognize the purpose and meaning of the process.
   c. Security practices for smart cities not related to IoT security are excluded.
   d. Explicit and implicit IoT security practices for smart cities from models were included.

   The output of this step consisted of the 45 IoT security practices presented in Table II. Most of these security practices are redundant and need to be merged to produce common IoT security practices for smart cities. The next step discusses how the IoT security practices were merged and grouped for smart cities.
3. **Proposing common IoT security practices*:*** This step explains how the 45 IoT security practices are grouped into categories based on their similarities in meaning and activities, and then proposes common IoT security practices. The same approaches have been suggested in [63-65]. The particular study proposes eight categories of IoT security practices, as given in Table IV. The next step is to establish relationships between the IoT security practices proposed in the present step.
4. **Identifying relationships among IoT security practices:** This step recognizes the connections among the practices involved in the proposed IoTSM. It was discovered that three types of UML relationships are commonly found in data models: associations, specializations/generalizations, and aggregations. A relationship of association generally indicates that a class retains a relationship with another class to fulfill one of its missions [67]. On the other hand, the specialization/generalization relationship connects a subclass to its superclass, and vice versa. It refers to the inherited attributes and operations of a superclass from its subclass over the superclass [65]. Finally, aggregation relationships are typically characterized by implied ownership [67]. For example, IoT Device Security practice has specializations along with IoT Security Training and Awareness, IoT Security Monitoring and Incident Response, and IoT Network Security practices. The Legal and Regulatory Compliance practice has an association relationship with IoT Privacy and Consent Management Practice. And IoT Device Security practice has aggregation relationship with IoT Security Training and Awareness, IoT Security Monitoring and Incident Response, and IoT Network Security practices. Figure 2 displays the structure of IoTSM.

TABLE II. IDENTIFYING AND SELECTING THE IOT SECURITY MODELS

Year	**Ref**	**Practices that enhance IoT security solutions for smart cities**						
		Authentication and authorization	**Device management**	**Intrusion detection and prevention**	**Device integrity**	**Secure communication**	**Secure data storage**	**Security incident response**
2018	[11]	√	√	×	√	√	×	×
2018	[12]	×	√	×	√	√	×	√
2019	[13]	√	√	×	√	√	×	√
2019	[14]	√	×	√	√	√	√	×
2020	[17]	√	√	×	×	×	√	√
2020	[18]	×	×	√	×	√	√	√
2021	[20]	√	√	√	×	√	×	√
2022	[61]	√	√	×	×	√	√	×
2022	[23]	√	√	√	×	×	×	√
2022	[24]	√	√	√	√	√	√	×
2023	[27]	√	√	√	×	×	√	×
2023	[29]	√	√	√	√	√	×	√
2023	[31]	√	√	√	×	×	×	√
2023	[32]	√	√	×	√	√	×	×
2023	[35]	×	√	×	√	√	√	×
2023	[36]	√	√	×	×	√	√	√

TABLE III. EXTRACTED IOT SECURITY PRACTICES

Year	**Ref**	**Extracted IoT Security Practices**
2018	[11]	Access Control, Mobile Device Management, IT Asset Management
2018	[12]	Configuration Management, Intrusion Detection and Prevention,
2019	[13]	Authentication, authorization, Verification, IoT Security, Smart city
2019	[14]	Device Integrity, Integrity Assurance, Data Integrity,
2020	[17]	Credential Management, Identification, Authorization Management,
2020	[18]	Secure Communication Channels, Secure Communication Network, Secure Data Storage, Data Encryption, Secure Data Storage Solutions
2021	[20]	Incident Response Process, Incident Response Team,
2022	[61]	Device Management, Intrusion Prevention Systems, Network Intrusion Prevention System,
2022	[23]	Device Integrity Control, Secure Communication, Secure Communication Protocols,
2022	[24]	Host Intrusion Prevention System, Threat Detection and Response,
2023	[27]	Incident Response Strategy, Incident Response Management
2023	[29]	Secure Communication Gateway, Secure Communication Architecture
2023	[31]	Remote Device Management, Cybersecurity Measures, Device Integrity Monitoring
2023	[32]	Intrusion Detection Systems, Device Management Solutions
2023	[35]	Data Security Solutions, Data Confidentiality
2023	[36]	Data Integrity, Security Incident Response, Incident Response Plan

TABLE IV. PROPOSED COMMON IOT SECURITY PRACTICES

Proposed common IoT security practices	**Description**
IoT Device Security	This practice aims to secure not only the physical components, but also the digital components of IoT devices. Several measures are included in this process, such as encryption, biometric authentication, secure booting, and an encrypted method of communicating between computers.
IoT Network Security	It is crucial for protecting sensitive data and ensuring that IoT mechanisms interact with one another. Among these are secure routing protocols, firewalls, encryption, and intrusion detection systems.
IoT Data Management	It is important for the protection of IoT data and ensuring secrecy. It encompasses access control, data anonymization, data encoding, and data hiding.
User Authentication	This practice is an important component of the IoT security strategy. There is a focus on applying secure verification approaches, such as multi-factor verification, one-time passwords, and secure biometric identification along with multi-factor authentication techniques.
IoT Security Monitoring and Incident Response	Monitoring and responding to security incidents are essential to maintaining a secure IoT environment. This component encompasses intrusion detection systems, security analytics, incident response plans, and periodic security assessments.
Legal and Regulatory Compliance	Compliance with legal and regulatory requirements is essential to smart cities. This component focuses on ensuring compliance with data protection laws, privacy regulations, and industry-specific standards.
IoT Privacy and Consent Management	Privacy and consent management are crucial to ensuring the ethical use of IoT data. This component covers data consent mechanisms, data retention policies, and data anonymization techniques.
IoT Security Training and Awareness	Security awareness and training are essential to promoting a culture of security in smart cities. This component includes awareness campaigns, security awareness training, and employee education programs

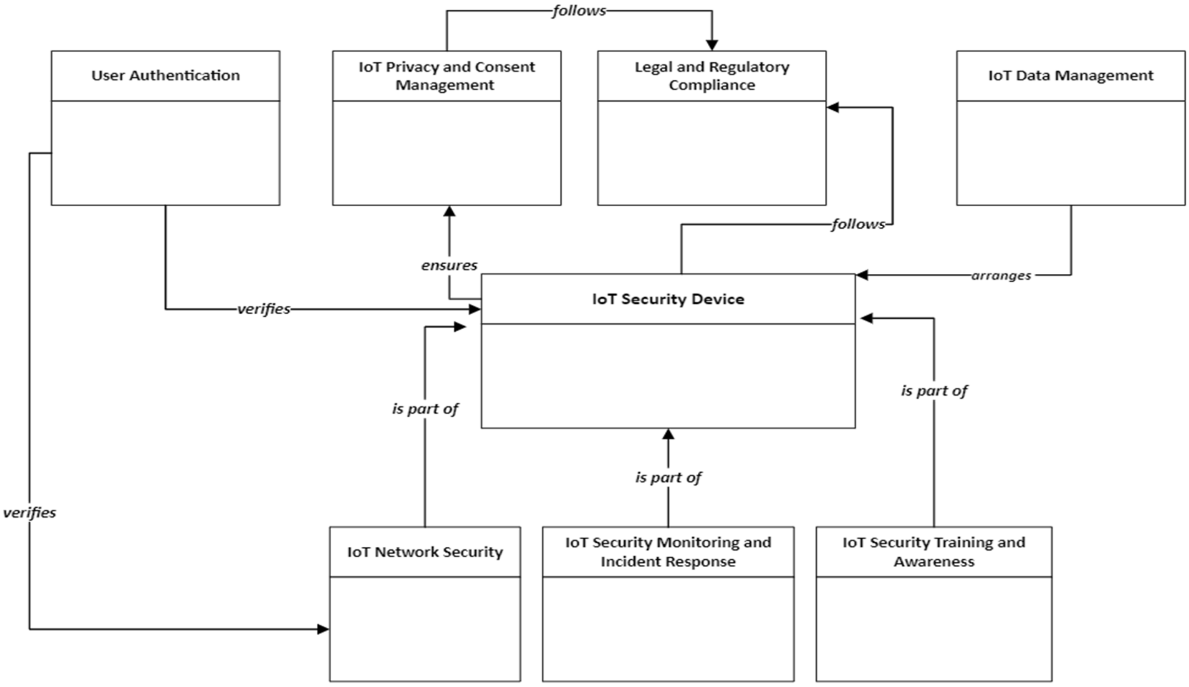

Fig. 2. The proposed IoTSM for smart cities.

IV. RESULTS AND DISCUSSION

To secure smart cities, providing comprehensive IoT security solutions is necessary. In addition, to reduce cyber threats, authentication and access controls should be strengthened, data should be encrypted, patches and updates should be conducted regularly, intrusion detection and prevention systems should be implemented, networks should be segmented, and secure communication channels should be established. Proposed IoT security models for smart cities have considered seven aspects of security: authentication and authorization, device management, intrusion detection and prevention, device integrity, secure communication, secure data storage, and response to security incidents, as presented in Table V. For example, authors in [10, 11, 13, 14, 16, 20-32, 36, 37, 61] discussed the security of IoT for smart cities from the authentication and authorization perspectives, whereas authors in [11-13, 17, 20, 22-25, 27, 29, 31, 32, 35-37, 61] explored it from the perspective of device management. In [14, 15, 18-25, 27, 29-31, 38, the authors investigated the intrusion detection and prevention techniques to improve the IoT security for smart cities. Researchers in [11-14, 16, 24, 29, 32, 35] examined the IoT security for smart cities from the device integrity perspective. The secure communication for IoT security in smart cities was covered in [9, 11-14, 18-20, 24-26, 29, 30, 32, 35-38, 61. Securing data storage to enhance IoT security solutions for smart cities was discussed in [14, 16-18, 21, 24, 27, 30, 35, 36, 61. Finally, authors in [12, 13, 15, 17, 18, 20, 23, 25, 29, 31, 36 studied the IoT security for smart cities from a security incident response perspective. Table V exhibits the analysis of IoT security models proposed in the literature for smart cities from different security aspects.

According to Figure 5, the existing IoT security models for smart cities are primarily focused on authentication and authorization security practices. These security measures are heavily emphasized, as they play a vital role in protecting sensitive data and ensuring authorized access to IoT systems. The second security aspect is secure communication and device management. This aspect involves ensuring the secure transmission of information between IoT devices and the cloud, as well as the management of IoT devices and their resources. This is crucial in order to maintain a secure ecosystem and prevent unauthorized access or manipulation of IoT components. Overall, the emphasis on authentication and authorization security practices indicates that they are considered to be key aspects of IoT security in smart cities. Additionally, the focus on secure communication and device management highlights the important contribution of these additional security measures in ensuring the integrity and security of IoT systems.

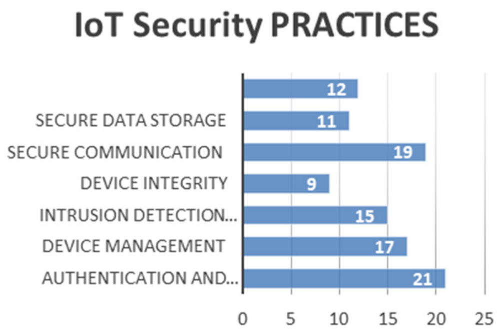

Fig. 3. The coverage of IoT security practices in the analyzed models.

TABLE V. COMPARISON OF THE EXISTING IOT SECURITY MODELS WITH THE DEVELOPED IOTSM

Year	**Existing IoT security models**	**Proposed practices to enhance IoT security solution for smart cities**						
		Authentication and Authorization	**Device Management**	**Intrusion Detection and Prevention**	**Device Integrity**	**Secure Communication**	**Secure Data Storage**	**Security Incident Response**
2018	[9]	×	×	×	×	√	×	×
2018	[10]	√	×	×	×	×	×	×
2018	[11]	√	√	×	√	√	×	×
2018	[12]	×	√	×	√	√	×	√
2019	[13]	√	√	×	√	√	×	√
2019	[14]	√	×	√	√	√	√	×
2019	[15]	×	×	√	×	×	×	√
2020	[16]	√	×	×	√	×	√	×
2020	[17]	√	√	×	×	×	√	√
2020	[18]	×	×	√	×	√	√	√
2020	[19]	×	×	√	×	√	×	×
2021	[20]	√	√	√	×	√	×	√
2022	[61]	√	√	×	×	√	√	×
2022	[21]	√	×	√	×	×	√	×
2022	[22]	√	√	×	×	×	×	×
2022	[23]	√	√	√	×	×	×	√
2022	[24]	√	√	√	√	√	√	×
2022	[26]	√	×	√	×	√	×	×
2023	[27]	√	√	√	×	×	√	×
2023	[28]	√	×	×	×	×	×	×
2023	[29]	√	√	√	√	√	×	√
2023	[30]	×	×	√	×	√	√	×
2023	[31]	√	√	√	×	×	×	√
2023	[32]	√	√	×	√	√	×	×
2023	[34]	√	×	×	×	×	×	×
2023	[35]	×	√	×	√	√	√	×
2023	[36]	√	√	×	×	√	√	√
2024	[37]	√	√	×	×	√	×	×
2024	[38]	×	×	√	×	√	×	×

Based on the above analysis, the IoT security field is experiencing several challenges and issues due to the current state of technology. For example, implementing IoT security solutions in smart cities is both heterogeneous and complex, due to the variety of connected devices and the various IoT communication procedures used in smart cities, as well as the differences in connected devices and systems in these cities. In addition to managing IoT security in smart cities, a second challenge is to ensure that the access to data is authenticated and authorized. IoT security in smart cities cannot be achieved simply with traditional access control. Therefore, a strong authentication method, such as public key infrastructure or multifactor authentication should be considered for IoT security in smart cities. IoT security in smart cities is affected by many other factors, involving data privacy and confidentiality, scalability and performance, vulnerability assessment, and patch management. Furthermore, the redundant IoT security processes, tasks, procedures, models, and frameworks that are produced are duplicated within each other, which leads to other challenges and issues. Therefore, IoTSM for smart cities was developed to solve the heterogeneity, complexity, and ambiguity of the IoT security field among domain security practitioners. It covered many abstract IoT security practices, which can be employed to secure the privacy and integrity of the smart city's components.

However, adopting IoTSM faces many challenges, namely the compatibility with the existing infrastructure, scalability and performance, and data privacy and ethical considerations. One of the primary limitations in adopting the developed IoT security metamodel in different smart city contexts is compatibility. Different smart cities may have diverse technological infrastructure, including different types of IoT devices, communication protocols, and cybersecurity solutions. Other challenges are scalability and performance. As smart cities continue to grow and expand, the number and complexity of IoT devices and networks increase. The metamodel must accommodate this growth without compromising efficiency or functionality. Data privacy and ethical considerations are paramount in the smart city contexts. The developed IoT security metamodel must address these concerns and ensure the protection of sensitive data.

In addition, this study emphasizes the importance of assessing the proposed model's contributions based on metrics, such as security level, secure connections, secure storage, and intrusion detection accuracy. One of the primary contributions of the proposed IoT security model is the enhancement of the security of IoT devices. The model utilizes a metamodeling technique in order to ensure a robust and systematic approach to securing the infrastructures of future smart cities. The metamodeling approach aids in identifying security requirements, mapping them to IoT systems, and then designing secure architectures and protocols. The proposed model also plays a significant role in certifying safe internet connections in smart cities. Metamodeling has been introduced to the industry as a method for identifying and prioritizing the secure communication channels needed for the different IoT applications. A security model designed to protect IoT devices, and the central system engages encryption techniques, authentication mechanisms, secure protocols, and verification mechanisms to ascertain resilient communication between these devices and the central system. To guarantee the confidentiality of private information, data protection steps are taken to prevent unauthorized parties from accessing, tampering with, or intercepting communication or data. In addition to its strong focus on secure storage, the proposed IoT security model features safe communication. Due to the increasing amount of data generated by IoT devices in smart cities, securing these data has become of paramount importance, especially in the long run. With metamodeling, developers can incorporate secure storage mechanisms into their applications, such as encryption, access controls, and authentication. Metamodeling helps identify specific intrusion detection algorithms and rules, which enhances detection accuracy. The proposed security model can pinpoint and respond to cyber threats in real-time by analyzing patterns, anomalies, or suspicious activities. In this way, it minimizes the impact of a potential security breach.

V. CONCLUSION

There is no doubt that IoT security is a very important aspect of the IoT world in terms of protecting users' privacy, device infrastructure, and data integrity as well as guaranteeing that the services offered by the IoT ecosystem are always available, regardless of the time or place. Several researchers who have attempted to identify the most suitable security solutions to promote the adoption of IoT in smart cities. However, its implementation still requires a comprehensive approach to succeed. This study introduced a highly abstract IoT security metamodel, called IoTSM, applicable to smart cities. The developed IoTSM provides a complete framework for smart cities. By combining most of the existing IoT security practices, it offers a comprehensive approach to addressing the unique security challenges posed by IoT technologies in urban environments. With the widespread adoption of IoT solutions, smart cities need to prioritize security to ensure individuals, infrastructure, and sensitive data. Several tasks need to be completed in the future to validate the completeness of the developed IoTSM. In addition, further research is required to demonstrate IoTSM effectiveness in real scenarios.

REFERENCES

[1] K. M. Alam, M. Saini, and A. E. Saddik, "Toward Social Internet of Vehicles: Concept, Architecture, and Applications," *IEEE Access*, vol. 3, pp. 343–357, 2015, https://doi.org/10.1109/ACCESS.2015.2416657.

[2] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, https://doi.org/10.48084/etasr.6195.

[3] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in *Internet Technologies and Applications*, Wrexham, UK, Sep. 2015, pp. 219–224, https://doi.org/10.1109/ITechA.2015.7317398.

[4] K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: from a heterogeneous network integration perspective," *IEEE Network*, vol. 30, no. 2, pp. 102–108, Mar. 2016, https://doi.org/10.1109/MNET.2016.7437031.

[5] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," *IEEE Access*, vol. 7, pp. 54508–54521, 2019, https://doi.org/10.1109/ACCESS.2019.2913438.

[6] R. Geisler, M. Klar, and C. Pons, "Dimensions and Dichotomy in Metamodeling," in *3rd BCS-FACS Northern Formal Methods Workshop*, Ilkley, UK, Sep. 1998, pp. 1–20, https://doi.org/10.14236/ewic/NFM1998.10.

[7] A. Alshammari, "A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11445–11450, Aug. 2023, https://doi.org/10.48084/etasr.6091.

[8] J. Whittle, "Workshops and Tutorials at the UML 2002 Conference," in *International Conference on Model Driven Engineering Languages and Systems*, Dresden, Germany, Oct. 2002, pp. 442–447, https://doi.org/10.1007/3-540-45800-X_34.

[9] R. M. S. Martins, "Secure and High Performance Framework for Smart Cities Based on Iot," M.S. thesis, Universidade do Minho, 2018.

[10] A. Fayad, B. Hammi, and R. Khatoun, "An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach," in *Third International Conference on Security of Smart Cities, Industrial Control System and Communications*, Shanghai, China, Oct. 2018, pp. 1–7, https://doi.org/10.1109/SSIC.2018.8556668.

[11] L. Prathibha and K. Fatima, "Exploring Security and Authentication Issues in Internet of Things," in *Second International Conference on Intelligent Computing and Control Systems*, Madurai, India, Jun. 2018, pp. 673–678, https://doi.org/10.1109/ICCONS.2018.8663111.

[12] R. Bellefleur and D. Wang, "IoT-Enabled Smart City Security Considerations and Solutions," 2018, [Online]. Available: https://repository.library.georgetown.edu/handle/10822/1053223.

[13] M. A. Rashid and H. H. Pajooh, "A Security Framework for IoT Authentication and Authorization Based on Blockchain Technology," in *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)*, Rotorua, New Zealand, Aug. 2019, pp. 264–271, https://doi.org/10.1109/TrustCom/BigDataSE.2019.00043.

[14] J. C. Ware, "Secure Authentication Mechanisms for Smart City IoT Infrastructure," M.S. thesis, Utica College, Utica, NY, USA, 2019.

[15] S. Anawar, N. Zakaria, Z. Masud, M. Zulkiflee, N. Harum, and R. Ahmad, "IoT Technological Development: Prospect and Implication for Cyberstability," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 2, pp. 428–437, Jan. 2019, https://doi.org/10.14569/IJACSA.2019.0100256.

[16] S. M. Muzammal and R. K. Murugesan, "A Study on Secured Authentication and Authorization in Internet of Things: Potential of Blockchain Technology," in *International Conference on Advances in Cyber Security*, Penang, Malaysia, Aug. 2019, pp. 18–32, https://doi.org/10.1007/978-981-15-2693-0_2.

[17] R. M. A. Mohammad and M. M. Abdulqader, "Exploring Cyber Security Measures in Smart Cities," in *21st International Arab Conference on Information Technology*, Giza, Egypt, Nov. 2020, pp. 1–7, https://doi.org/10.1109/ACIT50332.2020.9300050.

[18] N. Chaabouni, "Intrusion detection and prevention for IoT systems using Machine Learning," Ph.D. dissertation, Universite de Bordeaux, Nouvelle-Aquitaine, France, 2020.

[19] T. Mudawi, "IoT-HASS: A Framework For Protecting Smart Home Environment," Ph.D. dissertation, Dakota State University, Madison, WI, USA, 2020.

[20] D. M. Mendez Mena, "Blockchain-based security framework for the internet of things and home networks," Ph.D. dissertation, Purdue University, West Lafayette, IN, USA, 2021.

[21] M. Asif, Z. Aziz, M. Bin Ahmad, A. Khalid, H. A. Waris, and A. Gilani, "Blockchain-Based Authentication and Trust Management Mechanism

for Smart Cities," *Sensors*, vol. 22, no. 7, Jan. 2022, Art. no. 2604, https://doi.org/10.3390/s22072604.

[22] A. Mohammad, H. Al-Refai, and A. A. Alawneh, "User Authentication and Authorization Framework in IoT Protocols," *Computers*, vol. 11, no. 10, Oct. 2022, Art. no. 147, https://doi.org/10.3390/computers11100147.

[23] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: technologies, applications, and challenges," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 8, pp. 10517–10553, Aug. 2023, https://doi.org/10.1007/s12652-022-03707-1.

[24] A. Bhardwaj *et al.*, "IIoT: Traffic Data Flow Analysis and Modeling Experiment for Smart IoT Devices," *Sustainability*, vol. 14, no. 21, Jan. 2022, Art. no. 14645, https://doi.org/10.3390/su142114645.

[25] U. Khalil, O. A. Malik, M. Uddin, and C.-L. Chen, "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*, vol. 22, no. 14, Jan. 2022, Art. no. 5168, https://doi.org/10.3390/s22145168.

[26] W. Fei, "Raspberry House: An Intrusion Detection And Prevention System For Internet Of Things (IOT)," M.S. thesis, Dalhousie University, Halifax, NS, Canada, 2022.

[27] M. Polychronaki, D. G. Kogias, H. C. Leligkou, and P. A. Karkazis, "Blockchain Technology for Access and Authorization Management in the Internet of Things," *Electronics*, vol. 12, no. 22, Jan. 2023, Art. no. 4606, https://doi.org/10.3390/electronics12224606.

[28] S. Alghamdi, A. Albeshri, and A. Alhusayni, "Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager," *Electronics*, vol. 12, no. 17, Jan. 2023, Art. no. 3721, https://doi.org/10.3390/electronics12173721.

[29] S. Ahmed and M. Khan, "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*, vol. 13, no. 9, pp. 1–17, Sep. 2023.

[30] U. A. Usmani, A. Happonen, and J. Watada, "Secure Integration of IoT-Enabled Sensors and Technologies: Engineering Applications for Humanitarian Impact," in *5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications*, Istanbul, Turkiye, Jun. 2023, pp. 1–10, https://doi.org/10.1109/HORA58378.2023.10156740.

[31] C. Zhonghua, S. B. Goyal, and A. S. Rajawat, "Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing," *The Journal of Supercomputing*, vol. 80, no. 2, pp. 1396–1425, Jan. 2024, https://doi.org/10.1007/s11227-023-05517-4.

[32] A. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques," *Mathematics*, vol. 11, no. 9, Jan. 2023, Art. no. 2073, https://doi.org/10.3390/math11092073.

[33] A. S. Alraddadi, "A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11505–11510, Aug. 2023, https://doi.org/10.48084/etasr.6128.

[34] S. Thavamani and C. Nandhini, "Major Security Issues and Data Protection in Cloud Computing and IoT," in *Intelligent Techniques for Cyber-Physical Systems*, 1st Edition., Boca Raton, FL, USA: CRC Press, 2023, pp. 317–336.

[35] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing," *The Journal of Supercomputing*, vol. 80, no. 3, pp. 3738–3816, Feb. 2024, https://doi.org/10.1007/s11227-023-05616-2.

[36] S. C. Avik *et al.*, "Challenges in Blockchain as a Solution for IoT Ecosystem Threats and Access Control: A Survey." arXiv, Nov. 26, 2023, https://doi.org/10.48550/arXiv.2311.15290.

[37] A. K. Tyagi, "Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications," in *AI and Blockchain Applications in Industrial Robotics*, Hershey, PA, USA: IGI Global, 2024, pp. 171–199.

[38] I. U. Khan, M. Ouaissa, M. Ouaissa, Z. A. E. Houda, and M. F. Ijaz, *Cyber Security for Next-Generation Computing Technologies*. Boca Raton, FL, USA: CRC Press, 2024.

[39] A. M. Rashad Al-dhaqm and M. A. Nagdi, "Detection and Prevention of Malicious Activities on RDBMS Relational Database Management Systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, Sep. 2012.

[40] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, S. B. A. Razak, A.-H. M. Emara, and D. S. Khafaga, "Towards Development of a High Abstract Model for Drone Forensic Domain," *Electronics*, vol. 11, no. 8, Jan. 2022, Art. no. 1168, https://doi.org/10.3390/electronics11081168.

[41] A. M. R. Al- Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in *International Symposium on Biometrics and Security Technologies*, Kuala Lumpur, Malaysia, Aug. 2014, pp. 322–327, https://doi.org/10.1109/ISBAST.2014.7013142.

[42] A. Al-Dhaqm, S. H. Othman, W. M. S. Yafooz, and A. Ali, "Review of Information Security Management Frameworks," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 69–80.

[43] M. Salem, S. H. Othman, A. Al-Dhaqm, and A. Ali, "Development of Metamodel for Information Security Risk Management," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 243–253.

[44] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 81–92.

[45] M. Saleh *et al.*, "A Metamodeling Approach for IoT Forensic Investigation," *Electronics*, vol. 12, no. 3, Jan. 2023, Art. no. 524, https://doi.org/10.3390/electronics12030524.

[46] A. M. R. Al-Dhaqm, "SimplifiedI Database Forensic Invetigation Using Metamodeling Approach," Ph.D. dissertation, University of Technology Malaysia, Johor, Malaysia, 2019.

[47] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," in *4th International Conference on Future Internet of Things and Cloud*, Vienna, Austria, Aug. 2016, pp. 356–362, https://doi.org/10.1109/FiCloud.2016.57.

[48] V. Kebande and H. Venter, "Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution," in *11th International Conference on Cyber Warfare and Security*, Boston, MA, USA, Mar. 2016, pp. 399–406.

[49] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. Hajar Othman, "Face Validation of Database Forensic Investigation Metamodel," *Infrastructures*, vol. 6, no. 2, Feb. 2021, Art. no. 13, https://doi.org/10.3390/infrastructures6020013.

[50] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020, https://doi.org/10.1109/ACCESS.2020.3014615.

[51] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, https://doi.org/10.1109/ACCESS.2020.3000747.

[52] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020, https://doi.org/10.1109/ACCESS.2020.3008696.

[53] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," *Forensic Science International: Reports*,

vol. 2, Dec. 2020, Art. no. 100122, https://doi.org/10.1016/j.fsir.2020.100122.

[54] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model Derivation System to Manage Database Forensic Investigation Domain Knowledge," in *IEEE Conference on Application, Information and Network Security*, Langkawi, Malaysia, Nov. 2018, pp. 75–80, https://doi.org/10.1109/AINS.2018.8631468.

[55] A. Aldhaqm, S. A. Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 12, no. 4, pp. 386–394, Feb. 2016, https://doi.org/10.19026/rjaset.12.2377.

[56] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of Common Concepts for the Mobile Forensics Domain," in *International Conference of Reliable Information and Communication Technology*, Johor Bahru, Malaysia, Apr. 2017, pp. 141–154, https://doi.org/10.1007/978-3-319-59427-9_16.

[57] A. Ali, S. Razak, S. Othman, and M. Arafat, "Towards Adapting Metamodeling approach for the Mobile Forensics Investigation Domain," in *1st International Conference on Innovation in Science and Technology*, Kuala Lumpur, Malaysia, Apr. 2015, pp. 364–368.

[58] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common Investigation Process Model for Internet of Things Forensics," in *2nd International Conference on Smart Computing and Electronic Enterprise*, Cameron Highlands, Malaysia, Jun. 2021, pp. 84–89, https://doi.org/10.1109/ICSCEE50312.2021.9498045.

[59] A. Alshammari, "Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 7, pp. 767–774, 2023, https://doi.org/10.14569/IJACSA.2023.0140784.

[60] F. Ullah, C.-M. Pun, O. Kaiwartya, A. S. Sadiq, J. Lloret, and M. Ali, "HIDE-Healthcare IoT Data Trust ManagEment: Attribute centric intelligent privacy approach," *Future Generation Computer Systems*, vol. 148, pp. 326–341, Nov. 2023, https://doi.org/10.1016/j.future.2023.05.008.

[61] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "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*, vol. 10, pp. 76805–76823, 2022, https://doi.org/10.1109/ACCESS.2022.3189998.

[62] S. Kelly and R. Pohjonen, "Worst Practices for Domain-Specific Modeling," *IEEE Software*, vol. 26, no. 4, pp. 22–29, Jul. 2009, https://doi.org/10.1109/MS.2009.109.

[63] A. Al-dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," *PLOS ONE*, vol. 12, no. 2, Feb. 2017, Art. no. e0170793, https://doi.org/10.1371/journal.pone.0170793.

[64] A. Ali, S. Razak, S. Othman, R. Marie, A. Al-dhaqm, and M. Nasser, "Validating Mobile Forensic Metamodel Using Tracing Method," in *Advances on Intelligent Informatics and Computing*, New York, NY, USA: Springer, 2022, pp. 473–482.

[65] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *International Journal of Computer Science and Network Security*, vol. 8, no. 10, pp. 163–169, 2008.

[66] R. Ibrahim, N. S. Leng, R. C. M. Yusoff, G. N. Samy, S. Masrom, and Z. I. Rizman, "E-learning acceptance based on technology acceptance model (TAM)," *Journal of Fundamental and Applied Sciences*, vol. 9, no. 4S, pp. 871–889, 2017, https://doi.org/10.4314/jfas.v9i4S.50.

[67] D. Pilone and N. Pitman, *UML 2.0 in a Nutshell*, Oreilly & Associates Inc, 2005.