Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions

Khairul Khalil Ishak, Noor Afiza Mat Razali, *Member, IAENG*, Nur Atiqah Malizan, Ghazali Sulong and Md Ghapar Md Johar

***Abstract* — Smart Cities rely on the Internet of Things (IoT) which is characterised by its diverse, distributed and complex infrastructure. These complexities present a range of cybersecurity challenges, making IoT security an area of great importance. The existing vulnerabilities in IoT leaves Smart Cities susceptible to various types of malicious attacks. These vulnerabilities can be exploited, ranging from opportunistic monetary gains to acts of terrorism that disrupt the systems of rival nations. The fact that conventional cybersecurity protection systems cannot be applied to IoT environments in Smart Cities is an additional challenge. The relationship between cybersecurity and IoT security of Smart Cities has become a crucial gap that must be thoroughly investigated. Hence, this paper extensively reviewing the existing literature concerning IoT applications in Smart Cities, with emphasis on cybersecurity and IoT security concerns. This study concludes that real-time threat detection and mitigation by leveraging fog computing and artificial intelligence models represent a significant advancement in securing IoT infrastructure against cyberattacks. The research outcomes contribute to the critical understanding of the challenges regarding IoT security and paves the way for advancing the research of cybersecurity within the Smart Cities ecosystem.**

Keywords—Smart Cities, cybersecurity, IoT security, computing

I. Introduction

Global cybersecurity threats in Smart Cities are becoming increasingly critical with the annual growth of device implementations in the Internet of Things (IoT) [1]–[8]. The widespread adoption of IoT devices in Smart Cities presents a considerable cybersecurity challenge as it provides opportunities for malicious actors to exploit the vulnerabilities of IoT devices. This exploitation may be aimed at disrupting public services, obtaining financial gains or even used for offensive purposes between conflicting nations. Such threats to the IoT system in Smart Cities can be viewed as a threat to national security.

Therefore, in-depth research on the vulnerabilities inherent in diverse IoT applications and their exploitation vectors within Smart Cities ecosystems is crucial for developing robust mitigation strategies and safeguarding these interconnected environments [9]. Studies have shown that the development of Smart Cities highly depends on the locality requirement of each city due to specific government conditions, geographical factors and needs of the community. Inadequate consideration of these factors leads to considerable challenges, rendering security implementations impossible, as no out-of-the-box solutions can be applied effectively [10]. Current conventional cybersecurity standards and frameworks do not directly address the security requirements of IoT system implementation in Smart Cities [11]. The absence of designated cybersecurity framework embedded with IoT applications consideration poses a significant threat to Smart Cities, which can have far-reaching consequences for the overall functionality of the urban environment. To mitigate these risks, researchers must highlight the limitations of current cybersecurity standards and frameworks by considering the unique security challenges of Smart Cities with additional emphasis on IoT in such context. This paper presents a review of published literature concerning the cybersecurity of Smart Cities and discusses why IoT security must consider the special requirements of Smart Cities, including multiple IoT systems and strategies needed for addressing the gap. This is due to the fact that each system serves a specific purpose, such as Smart Transportation Management, Smart Governance, Smart Energy, etc. [12]. The paper is organised as follows. Section 2 presents the methodology of this survey. Section 3 review the key components of Smart Cities, overview of IoT implementation, cybersecurity challenges and proposed solution as well as the strategy implementation suggested in the literature. Finally, Section 4 highlights the conclusion and future works.

II. Survey Methodology

For a comprehensive survey, articles published between the years of 2017 and 2023 in Scopus and Google Scholar were searched and selected. In this paper, state-of-the-art Smart Cities, cybersecurity and IoT were reviewed by focusing on the three-layered IoT architecture. Literature that addressed the implementation of IoT in Smart Cities was specifically examined. The search and selection sequences of the literature is shown in Figure 1. Certain keywords such as "smart cities" OR "smart city", "cybersecurity", "security", "IoT" and "computing" was used for the database search to determine the related literature. Approximately 505 literature articles were found in the initial search. Upon excluding redundant literature, non-article document types and non-English papers, a number of 176 articles were selected for the abstract content review.

Manuscript received August 11, 2023; revised May 7, 2024.

This work was supported in part by National Defence University of Malaysia (UPNM), Management and Science University (MSU) and Ministry of Higher Education Malaysia (MOHE) Fundamental Research Grant FRGS/1/2021/ICT07/UPNM/02/1.

Khairul Khalil Ishak is a PhD candidate at Management and Science University, Selangor, Malaysia (e-mail: khairul_khalil@msu.edu.my).

Noor Afiza Mat Razali is an Associate Professor at National Defence University of Malaysia, Kuala Lumpur, Malaysia (corresponding author phone: 603-90512548; e-mail: noorafiza@upnm.edu.my).

Nur Atiqah Malizan is a research assistant at National Defence University of Malaysia, Kuala Lumpur, Malaysia (atiqahmalizan@gmail.com).

Ghazali Sulong is a Professor at Management and Science University, Selangor, Malaysia (e-mail: ghazali@msu.edu.my).

Md Ghapar Md Johar is a Professor at Management and Science University, Selangor, Malaysia (e-mail: ghapar@msu.edu.my)

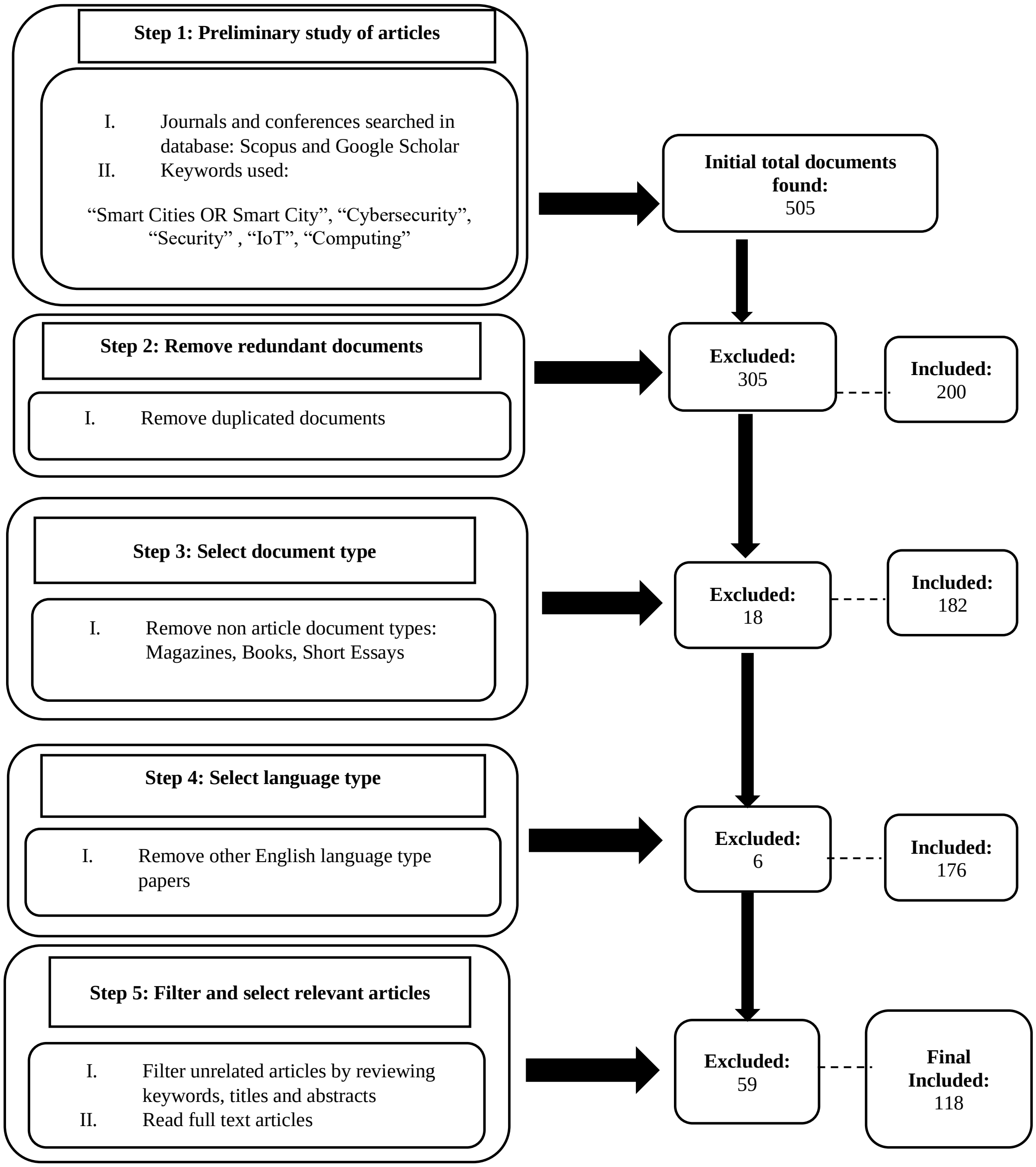
Step 1: Preliminary study of articles
I. Journals and conferences searched in database: Scopus and Google Scholar
II. Keywords used:
“Smart Cities OR Smart City”, “Cybersecurity”, “Security” , “IoT”, “Computing”
Initial total documents found:
505
Step 2: Remove redundant documents
I. Remove duplicated documents
Excluded:
305
Included:
200
Step 3: Select document type
I. Remove non article document types: Magazines, Books, Short Essays
Excluded:
18
Included:
182
Step 4: Select language type
I. Remove other English language type papers
Excluded:
6
Included:
176
Step 5: Filter and select relevant articles
I. Filter unrelated articles by reviewing keywords, titles and abstracts
II. Read full text articles
Excluded:
59
Final Included:
118

Fig 1. Research Methodology

After the abstract review, 118 were selected for a full analysis review.

In this study, we present a summary of the descriptive statistics, encompassing subject, year, and country-wise analyses, from the reviewed publication. The subject-wise classification is displayed in the chart in Figure 2, which indicates that most of the published research has been in the fields of computer science and engineering, science of energy, environment, business, and management. The number of research publications has also increased in the fields of decision sciences, materials science, and agricultural and biological sciences. This paper reviews the literature on the cybersecurity of Smart Cities and explains why Smart Cities’ cybersecurity requires other aspect of consideration and specific requirements, such as the necessity for multiple IoT systems and techniques to achieve this research objectives.

According to the year-by-year analysis, from 2015 onwards, a notable shift has emerged within IoT security research, with growing attention paid to incorporating the security demands of Smart Cities, characterized by their multifaceted and ever-expanding selection of IoT strategies and solutions. The number of articles increased significantly between 2018 and 2023. Figure 3 illustrates an exponential increase in publications released in 2019 compared to 2018, suggesting a developing trend in this field of study. Closer examination reveals a dual emphasis within the studies, encompassing both the specific concerns of IoT and Smart Cities alongside broader investigations into cybersecurity and computing architecture across diverse sectors. This trend likely stems from the expanding adoption of IoT technologies, driving an associated requirement for robust security solutions.

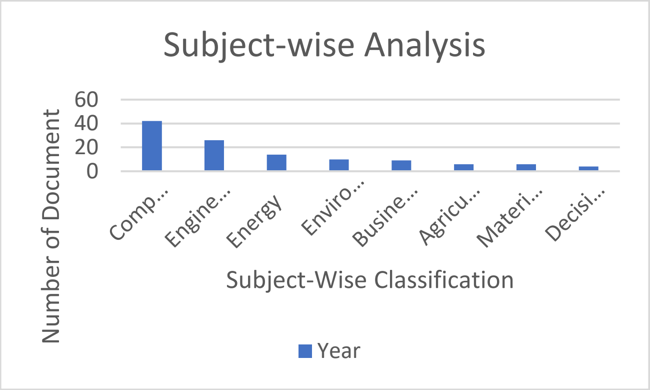

Fig 2. Subject-Wise Analysis

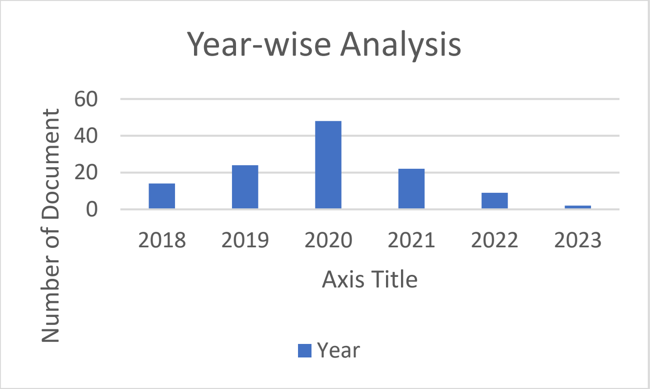

Fig 3. Year-Wise Analysis

The country-by-country analysis is shown in Figure 4, that reveals a pivotal trend with India leading the charge in research on tailoring IoT security for the unique demands of Smart Cities, characterized by their diverse set of systems and approaches. While the United States and United Kingdom follow closely with rising research output, this highlights the urgent need for intensified global efforts in Smart Cities IoT security to bolster robust security strategies. Asian nations, such as China, Malaysia, India, South Korea, and China, also significantly contributing to this field of study.

Three research questions (RQ) were adopted in this study and the review of articles was conducted according to the RQ. The research questions are as follows. RQ1: What are the existing IoT implementation in Smart Cities?; RQ2: How does the implementation of IoT in Smart Cities contribute to cybersecurity challenges?; RQ3: What are the standards and frameworks recommended for enhancing cybersecurity in Smart Cities?

III. Discussion

This paper defines the term ‘Smart Cities’ from a technological perspective. Throughout this paper, Smart Cities is characterised as a city that incorporates Information and Communication Technology (ICT) to model the physical and behavioural aspects of city elements and lifestyle into the digital environment.

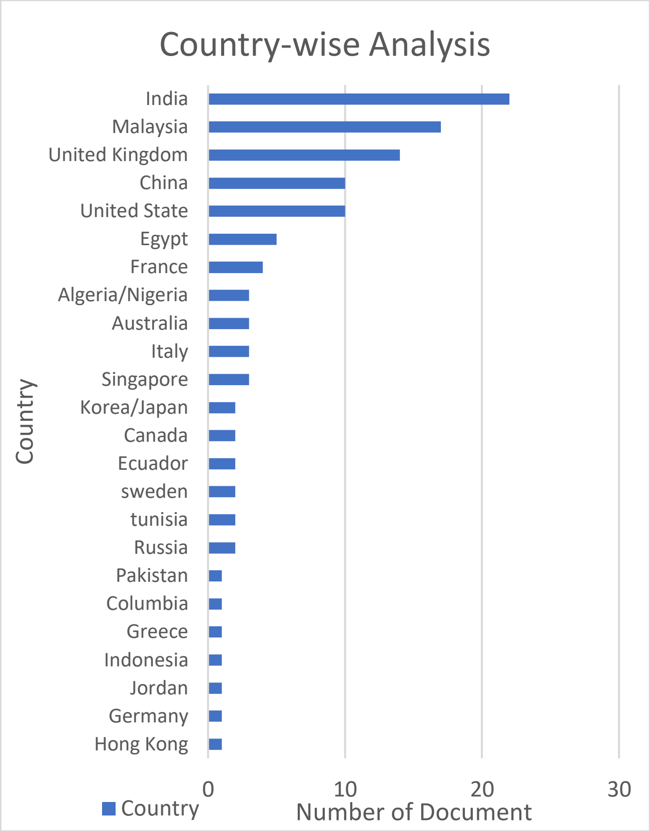

Fig 4. Country-wise Analysis

This is mainly accomplished through IoT devices and the enhancement of legacy apparatus through Internet connectivity, providing smart infrastructure and services that improve overall service efficiency and effectiveness for the wellbeing of citizens in such cities [13]–[17]. Meanwhile, IoT is defined as an architecture that enables internet connection to ‘things’ such as sensors, appliances, actuators, CCTV, traffic lights, in buildings, homes, transportation systems in [12], [18]–[21]. Historically, the concept of IoT was proposed by the Auto-ID Labs at the Massachusetts Institute of Technology (MIT) during the early 1990s [18]. The implementation of IoT systems had resulted in improved accessibility, flexibility and productivity of infrastructures and services in Smart Cities [22]. The concept of Smart Cities that derived from the combination and integration of smart infrastructures and systems (such as Smart Government, Smart Healthcare, Smart Transportation, etc) with IoT devices embedded as the core technology in numerous smart infrastructures and systems are discussed in [23], [24], [25], [26]. Firstly, to answer the RQ1 formulated for this study, this paper discusses the general architecture for IoT implementation in Smart Cities as shown in Figure 5. The general architecture is commonly based on a system of three technological layers: the device layer, the network layer and the application layer [8], [14], [27], [28]. The layers have three major functions: retrieving, transmitting, storing and processing data [29]. The first layer contains various IoT devices that include sensors, actuators and control devices. They are primarily used to detect surrounding environments and perform special functionalities, such as Smart Traffic Management or Smart Lighting for street lights to reduce energy waste [30], [31].

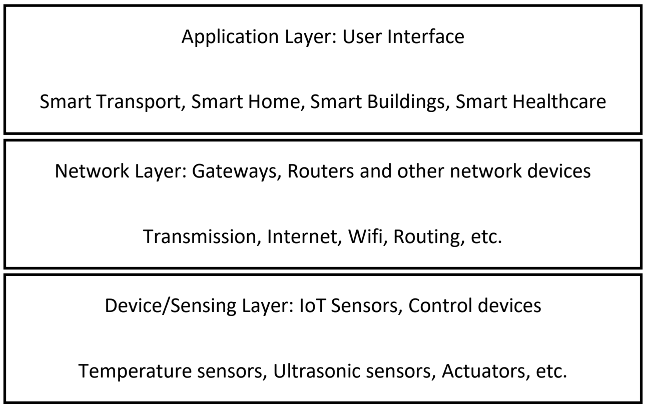
Application Layer: User Interface
Smart Transport, Smart Home, Smart Buildings, Smart Healthcare
Network Layer: Gateways, Routers and other network devices
Transmission, Internet, Wifi, Routing, etc.
Device/Sensing Layer: IoT Sensors, Control devices
Temperature sensors, Ultrasonic sensors, Actuators, etc.

Fig 5. IoT Architecture Layer

The network layer consists of network devices such as gateways, routers and specialised devices or servers that mainly use wireless network technologies (such as Wi-Fi, Cellular, NB-IoT, LoRa, SigFox, Zigbee, Bluetooth, etc.) that act as the communication interface to transmit data generated by IoT to the application layer for storage and processing [21], [27], [32]. The application layer is responsible for data storage, processing and visualisation [27], [28]. The interface to access the IoT data and systems, in the form of dedicated web or mobile applications, is provided in this layer [8].

A. *IoT Security Challenges and Cybersecurity*

IoT systems are seen as easy targets since their manufacturers and developers mainly emphasise usability, hardware resources and size rather than the security aspect of these systems [33], [34]. IoT security challenges are mostly due to the core characteristics of its implementation which are generally heterogeneous, inter-connected, ubiquitous and lack globally recognised security standards [14], [29], [35]–[37]. IoT devices have special security challenges in addition to the conventional cybersecurity issues normally faced by computers in a traditional organisational setting [27]. Researchers have discussed IoT security attacks according to the following categories: physical attacks [21], [38], network attacks [38], [31], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [33], application or software attacks [21], [38], data privacy, encryption, ethics and access control [34], [50].

Technological advancement comes with cybersecurity threats; thus, it is crucial to understand the specific requirements of Smart Cities, to secure IoT devices at all layers while also enhancing advanced threat detection technologies. To answer RQ2, this study is focusing to understand how implementation of the IoT in Smart Cities can contribute to cybersecurity challenges. First, we tailored the discussion towards understanding the threat and how the threat escalated to attacks. The threats on IoT web and mobile applications in the application layer are characterised and explained by the Open Web Application Security Project (OWASP), which is a renowned non-profit foundation that improves software security with its OWASP Top 10 Attack Surface Areas for IoT applications [42], [47], [51], [52]. Any vulnerabilities that arise from the OWASP Top 10 Attack Surface Areas for IoT could jeopardise the web or mobile applications for end-user implementations in the application layer since they can open doors for attackers as these applications are normally accessible from the Internet [37], [53].

Attacks on IoT devices have been widely reported in recent years [54]. BASHLITE, Mirai and its variants are an example of well-known malware used by attackers to infect IoT devices. They were later used for Distributed Denial of Service Attacks (DDoS) targeting websites of several large organisations [53], [55]. Attacks on IoT systems have significantly increased due to the global COVID-19 pandemic. This was due to the increased implementation of IoT systems throughout the world to cater for the digitalisation of services, especially in healthcare and e-commerce systems [56], [57]. The attacks exposed the vulnerabilities of IoT devices and the lack of awareness by users regarding IoT security [58]. These attacks can potentially allow malicious entities to compromise IoT devices in Smart Cities [8], making it possible for them to alter sensor configurations or take over traffic light management which may cause severe consequences to cities, such as traffic delays or accidents that can lead to loss of lives [9], [59]. The conventional network security system cannot be competently used in IoT environments. IoT devices have a different requirement nature and a diverse IoT network architecture compared to traditional computer networks [55], [60]–[62]. Side-Channel Attacks, for instance, can be used to exploit leaked information from the processors' microarchitecture of IoT devices, electromagnetic emanation or power utilisation to perform a malevolent activity.

In the network layer, software-related threats consist of Malicious Code Injection Attacks used by attackers to inject malware into IoT devices. This is normally accomplished during firmware or applications on the air upgrade [44]. Sleep Deprivation Attacks are another type of software attacks where malicious codes can execute loop programs that will consume the limited power source in IoT devices and deplete the battery, making them unavailable to perform their tasks [44]. Also, in the network layer, the key function is to provide communication services that transmit data collected by IoT devices through network devices and, in some cases, serve as a gateway for IoT devices to access the Internet to connect to the Cloud infrastructure or end-user applications [21], [28], [44]. Various technologies are used in this layer for the purpose of communication between IoT devices and other network devices [45]. Since the communication technologies used are numerous, security challenges in this layer include specific technological vulnerabilities, such as in Zigbee, where the symmetric keys used for encrypting communication are transferred in clear text during the initial connection of IoT devices [63]. Similar to the device/sensing layer, network devices can be installed in public areas which can be accessed by attackers, therefore, another challenge is the protection against signal jamming that denies communication in an IoT environment [64]–[67]. Since the network layer uses network protocols such as HTTP, TCP and UDP, the layer inherits common security threats from the traditional implementation of organisational networks, for instance, the Distributed Denial of Service (DDoS), Man in the Middle Attack (MITM), Spoofing, Sinkhole attack and Sybil attack [33], [36]. The DDoS attack is accomplished when multiple compromised systems are used to target a single system, typically a server or website, where the compromised systems send enormous amounts of requests for a resource to the server or website that may exceed 600 Gigabits of traffic per second. This causes a slow response time or even crashes the services in the server or website [33]. An example of a DDoS attack is a malware called Mirai, which emerged in September 2016. The attack compromised and used hundreds of thousands of IoT devices over the Internet to execute the DDoS, causing the inaccessibility of several websites, such as Netflix and Twitter [33], [41], [46], [68]. MITM, on the other hand, is where attackers sit in the middle between the communication of computers, or in this case, between the IoT devices' data transfer to secretly intercept the information in the network. The attackers can retrieve the intercepted information and, in some cases, manipulate the information in the data before it reaches the final recipient [21], [36], [65]. Due to limited computing, memory and power resources in most IoT devices, the IoT system does not perform encryption when transmitting the data, which makes MITM attacks very significant to IoT implementations. This is especially significant for Smart Cities where by altering data, attackers can send false information regarding critical data (such as from chemical sensors) that may lead to serious consequences [64]. In a Spoofing attack, a malicious IoT device will try to impersonate another valid IoT device by falsifying its identity. This can be done by altering the HTTP packet headers in order to disguise its original identity. If it succeeds, the attacker can portray himself as a legitimate user in order to gain access to data and transmission privileges [69]. The attacker may also gain access to transferred data and extend the attack as MITM or DDOS attacks in the IoT system by spoofing the IP address of the genuine IoT node and flood request packets to the servers in the Cloud infrastructure [22], [36]. In a Sinkhole attack, the attacker will advertise an artificial shortest routing path in the network with the intention to attract the nodes to route its data transmission traffic through the attacker node where it can drop or selectively forward packets in the network [27], [36], [60], [70]–[72]. A Sinkhole attack does not necessarily disrupt legitimate transmission within the network, but it can potentially examine the information within packets and only disrupt packets from certain nodes [43]. In a Sybil attack, the attacker tries to forge multiple numbers of IoT nodes using false IDs with the objective of taking control of any Peer-to-Peer communication within the network [36]. Sybil attacks can occur in the open communication medium. The attacker can exploit any leaked keys or identity information to potentially create a large number of fake IoT nodes that could, in turn, also act as authenticated nodes and execute malicious interactions to intentionally increase or decrease the reputation of nodes, such as for the Proof-of-Work (PoW) tasks in a blockchain system [73], [74], [75].

In the application layer, smart services are provided to end users [44]. The threats and security challenges in this layer are highly related to the challenges faced by common web or mobile applications, for example, software vulnerabilities, misconfiguration, lack of encryptions, weak authentication and authorisation mechanisms that may lead to access control attacks, DoS attacks, buffer overflow attacks, malware attacks, denial of services, phishing, traffic analysis attacks, MITM and exploitation of web application vulnerabilities [14], [27], [44], [66]. The summary in Table I highlights the IoT security attacks according to the specific layers due to IoT device implementations in Smart Cities that resulted in cybersecurity issues.

TABLE I. IOT SECURITY ATTACKS AND CHALLENGES

IoT Security Attacks
Physical Layer [14] [21][38] [53] [58]
Node Tampering RF Interference on RFID Malicious Node Injection Physical Damage Sleep Deprivation Social Engineering Jamming Malicious Substitution Sensing Tampering/Physical Damage Node Capture Cloning /Device Replication
Network Layer [14] [33][19] [21] [27] [31] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [53] [8], [14], [27], [28] [30][58] [60] [70] [71] [72] [63][72] [74] [75] [76]
Eavesdropping RFID cloning Spoofing Unauthorized attack Sinkhole Attack, Sleep Deprivation Attack Traffic Analysis DDos Attack MITM Attack Routing Information Attack IPsec Communication With Ipv6 Nodes Different Iot-Enabled Communication Protocols Collision Exhaustion Unfairness Spoofed, Altered Or Replayed Routing
Application/Software Layer [14][21] [38] [53][58] [54] [64] [74]
Malicious scripts Phishing attack, Cross-Site Request Forgery (CSRF) Viruses, Cross-Site Scripting (XSS) Worms and spyware Denial-of-Service (Dos) attacks Reverse-engineering, Elevation of privilege, Many logged-in users with the same credentials Stolen verifier Stolen/lost smart cards Application password guessing, Code execution, Structured Query Language (SQL) injection, Password change Buffer overflow Impersonation Memory corruption
Data Privacy [58] Identification, Localisation and Tracking, Profiling, Life-cycle Transitions, Linkage Inventory Attack
Encryption [28][58] Side Channel Attack, Cryptanalysis Attack
Ethics [58] Owner Identification, Public and Private Border Line, People’s life Attack
Access Control [68] [52] [73] [77] [78] [79] Access Control Management, Privilege Management

Besides, IoT devices have limited computational power, battery life, memory capacity and power supply, therefore, the conventional encryption methods used in PCs are not suitable for IoT devices [19]. Many IoT devices also implement and interact with physical environments, such as environmental sensors, traffic lights and security cameras, therefore, security challenges may not only arise from the digital realm but also from physical threats [34]. For instance, Node Capturing and Side-Channel Attacks are physical threats that can be maliciously used for IoT devices [27]. Node Capturing attack is done by replacing the genuine IoT device in the system with malicious nodes. The malicious node may be seen as part of the normal node but it is used by attackers to compromise the IoT system. To enhance the security of replacing the genuine node, researchers proposed a blockchain technology mechanism to strengthen the access control mechanism for IoT devices and establish a reliable and robust solution [73], [77], [78], [80]. In conclusion, the growing deployment of interconnected IoT devices in urban environments heightens vulnerability to cyber threats. This chapter highlights that IoT attacks have significant implications for the cybersecurity landscape within Smart Cities.

B. Implementation of Fog Computing to Mitigate IoT Constraints.

Since IoT systems have heterogeneous characteristics with very limited device resources, including low computing power and complex infrastructures, network protocols and communication technologies such as Lora, Sigfox and NB-IoT have been created [11], [27], [28], [81]–[83]. Most IoT systems use on-demand resources in the Cloud infrastructure for data storage, processing and analytic services [39]. The main reason for utilising the Cloud infrastructure is because a significant proportion of IoT devices are small in size and possess limited computing resources, memory capacity and data storage capabilities [84]. IoT devices normally generate large volumes of data and sometimes with high velocity that will require large storage space [85]–[87]. Generally, it makes more sense for organisations to design its IoT systems to offload the data storage and process onto the Cloud infrastructure rather than investing in on-premise full-capacity facilities that would cost much higher [88]. However, being fully reliant on Cloud will not always be a suitable solution for IoT systems, especially when it comes to security issues. This is due to the fact that the locations where the IoT devices are implemented are generally far from the physical Cloud infrastructure facilities. In some cases, they can even be in a different countries' system which could create latency in data processing and communication [89], [90]. Thus, this may not work well for IoT systems for latency-sensitive services, such as responses for Autonomous Vehicles or emergency alerts from medical devices in Smart Healthcare systems [72], [91], [92]. Due to the previously mentioned issues, some services (such as data storage, processing and analysis) for the IoT system that are latency sensitive can be implemented within the network layer in the IoT architecture [31] [93]. The literature reviewed in this study establishes that Fog computing provides high implementation potential in real applications of IoT environments, especially in Smart Cities. Fog computing is a term coined by CISCO [4], [93], [94] in CISCO’s Computing (2017) white paper. Fog computing is explained as the extension of the Cloud, with smaller resource capacities that sit between the IoT devices and the Cloud.

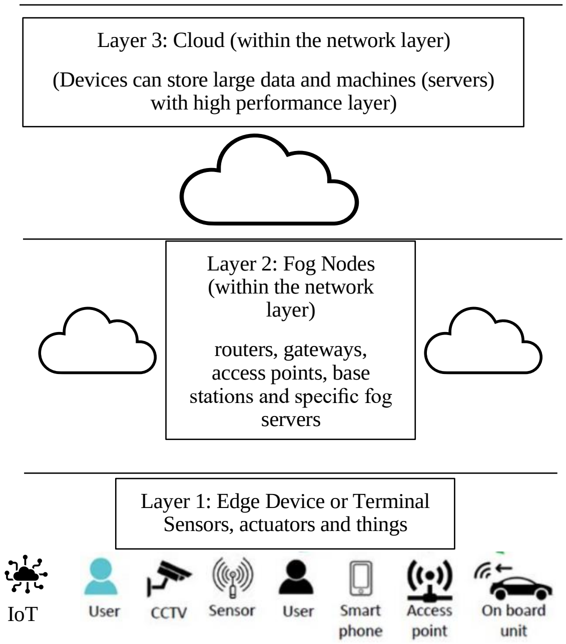
Layer 3: Cloud (within the network layer)
(Devices can store large data and machines (servers) with high performance layer)
Layer 2: Fog Nodes (within the network layer)
routers, gateways, access points, base stations and specific fog servers
Layer 1: Edge Device or Terminal Sensors, actuators and things
IoT
User
CCTV
Sensor
User
Smart phone
Access point
On board unit

Fig. 6. Fog Computing in IoT Architecture

Fog computing is recognized as the promising architecture that is gaining momentum for implementing IoT systems in Smart Cities [95]. The actual devices, also known as Fog nodes, are any devices with computing, storage and network connectivity capabilities that can be deployed in the IoT architecture’s network layer, either as part of gateway servers or as specialised servers [92], [93], [96]. Figure 6 presents Fog computing in IoT architectural implementations. Fog computing or also known as Fog nodes is mainly used to manage data produced by IoT in a locally manner that consist of a gateway, routers or dedicated servers that are near IoT for better data processing and reduced response latency, which is very essential for security [27], [97]. [28], [31], [24], [98], [99], [72], [40], [48]. Since most IoT devices have very limited hardware and software resources, the usual security measures implemented in normal computers cannot be implemented in IoT devices [44].

The Fog nodes can be located anywhere in the organisation's compound, on a power pole, beside the railway track, inside a vehicle or within an oil rig machinery [4], [100]. By using Fog computing, time-sensitive responses to IoT are realised by eliminating a round trip to the Cloud. This also makes it possible to lower network traffic by processing and filtering raw data in the Fog nodes and sending only the required data to the Cloud infrastructure for further data analysis and processing [40], [101]. In a way, Fog computing can also avoid the costly bandwidth for Internet data transfers from IoT devices to the Cloud by offloading gigabytes of network traffic from being transferred [102]. Simultaneously, Fog computing can further protect sensitive IoT data from being exposed during data transfer through the Internet by filtering it inside the walls of IoT implementations [4], [102], [103]. Overall, Fog computing can substantially reduce the workload and processing time needed in the Cloud. Thus, it can provide options to ease the drawbacks of Cloud services [96], [98], [104]. Similar to Fog computing, Edge computing is a range of networks and devices at or near IoT devices that process data.

Zhou et al. (2019) proposed a DDoS attack on industrial IoT operation mitigation approach using Fog computing [22]. The approach uses a firewall, IDS and Cloud to provide the three-level architecture for DDoS mitigation. Fog computing was used for several firewalls, the IDS was applied to detect DDoS attacks at the IoT device level, while the Cloud was used to consolidate the collected data from all IDS to provide an overall picture of the network traffic and control and management functionality to reduce false positives and increase the accuracy of attack detection. The proposed architecture can provide an easy implementation strategy regarding industrial IoT operation as it uses a firewall and signature-based IDS at the local level as well as centralised management using Cloud. However, it still lacks the validation of unknown attacks that require behaviour-based IDS analysis.

Researchers in [22], [27], [28], [72], [97], [99], [101], [105]–[107] proposed that IoT security measures must be implemented in Fog computing to overcome the difficulty of resource-constrained security measures during implementation in IoT devices.

Since Fog computing is at the same location or near IoT devices, the computing needs for security requirements (such as network traffic analysis for detecting malware in IDS) can be performed on the Fog nodes [98], [102], [105], [107], [108]. In [97], the authors proposed an IoT security framework to detect malicious nodes in the Fog computing environment. The framework provides security of Fog nodes rather than their common utilisation in the security of the overall IoT environment. The framework is based on Cloud solutions with the Markov model, IDS and Virtual Honeypot Device (VHD) as its components. The framework was tested using the IDS attack generator tool called Pytbull, introducing an interesting concept of securing Fog nodes from attacks. However, it will add complexity once integrated with the security of IoT devices. It would be preferable if Fog nodes are integrated as part of the overall security system in the IoT environment. A summary of the proposed applications of Fog computing for IoT security application is presented in Table II. Researchers examine its potential to mitigate bandwidth constraints by enabling localized data processing closer to the edge of the network and reduce the burden on centralized servers by optimizing resource utilization and enhancing scalability for IoT.

TABLE II. FOG COMPUTING IN IOT IMPLEMENTATION IN SMART CITIES

Articles	Details
[22]	• Applies the Fog computing concept in DDOS mitigation by allocating traffic monitoring and analysis work close to local devices • Coordinates and consolidates work to Cloud central servers to achieve fast response while at a low false alarm rate
[4] [84] [91] [93] [94] [100] [106] [107]	• Discuss the characteristics of Fog computing and Edge computing • Discuss Fog computing as a novel middleware architecture that enables data analytics for the IoT data • Fog computing represents the evolution of modern computing paradigms and its outstanding role as the glue between IoT Cloud and Edge computing
[89]	• Advantages/disadvantages of using Cloud-based ERP in the healthcare sector to improve efficiency and cost
[97]	• The proposed cybersecurity framework uses three technologies, the Markov model, Intrusion Detection System (IDS) and Virtual Honeypot Device (VHD), to identify malicious Edge devices in the Fog computing environment.
[101]	• Proposed a fog-assisted software-defined network (SDN) driven intrusion detection/prevention system (IDPS) for IoT networks
[102]	• Provides a comprehensive understanding of Fog privacy and security issue
[104][107][108]	• Investigates a workload allocation scheme in an IoT–Fog–Cloud cooperation system for reducing task service delay, aiming at satisfying as many as possible delay-sensitive IoT applications' quality of service (QoS) requirements
[20][109]	• Intrusion detection and anomaly detection in Fog computing
[110] [111]	• Integrates IoT with Cloud and Fog computing as an improved platform to support IoT Smart Cities applications using integrated architecture of the IoT-Fog-Cloud computing model

C. Models to Address Cybersecurity Challenges in Smart Cities

The literature suggests that the implementation of Fog computing has been shown to effectively support data analytics in the domains of Smart Cities and national security through the use of Artificial Intelligence (AI) models by employing both Machine Learning (ML) and Deep Learning (DL) techniques [111][112]. A study [113] has assessed ML techniques for traffic classification in Software-Defined Networking (SDN). The research identified various studies that used ML algorithms, including Support Vector Machine, Decision Tree, k-NN, CNN, Naive Bayes, etc.

It noted that a combination of ML techniques can improve classification accuracy and further highlighted that application-aware and application-type traffic classification will contribute to efficient network resource allocation and management. The literature also discussed ML and DL as vital solutions for providing detection and prediction to solve cybersecurity issues in Smart Cities. To discuss RQ3, IoT security strategy implementation advantages and drawback is discussed, as shown in Table III.

TABLE III. IOT SECURITY STRATEGY IMPLEMENTATION

Articles	Security Strategy	Advantage	Drawback
[114]	IDS framework uses ANN technique to detect compromised Fog nodes within IoT environment	- Detects attacks for Fog nodes - ANN for malicious traffic detection	- Attack testing does not use benchmarked data - Does not consider the complexity of real Fog nodes implementation
[20]	Hybrid approach IDS in IoT system using binary and multi-class classification	- Fast detection in binary classification - Multi-class classifiers can further classify the type of attack	- Dataset tested was not specifically for IoT systems - Real-world application must be validated
[22]	Mitigation for (DDoS) attacks on industrial IoT based on Fog computing architecture	- Uses conventional Firewall and signature-based IDS - Less implementation effort	- Only focuses on DDoS - Lack of behaviour-based IDS for unknown attacks
[49]	An intelligent intrusion detection system (I-IDS) to identify attacks in IoT network	- Tested on multiple Machine Learning techniques - High scalability potential	- Does not consider the complexity of real Fog nodes implementation - Unknown attacks are not well addressed
[72]	Distributed network attack detection for IoT systems using Fog nodes and Deep Learning	- Tested on multiple Deep Learning techniques - Tested on the 5 main publicly available datasets	- Does not consider the complexity of real Fog nodes implementation - Not tested using unsupervised Deep Learning techniques
[97]	IoT security framework to detect malicious nodes in the Fog computing environment	- Detects attacks on Fog nodes - Secures Fog nodes that are commonly used to secure IoT systems	- Attack testing did not use benchmarked data - Does not consider the complexity of real Fog nodes implementation
[50] [65][66][87] [99]	ML and DL-based analytics for IoT security challenges	- Efficient data analytics	- More testing ground needed to evaluate various techniques
[69] [74] [115]	Blockchain technology application to resolve IoT node identification and authentication	- Application of distributed identification and as a solution for authentication using blockchain	- Further testing needed to evaluate the application in real world environment
[109]	IoT network security framework using signature and anomaly-based attack detection	- Fast detection in the signature-based method - Holistic approach for detection	- Does not use commonly applied software for signature-based method. Real-world application must be validated.
[110]	IoT-Fog-Cloud model for detecting anomalies in IoT network	- Simple implementation using Machine Learning techniques - High scalability potential	- Does not consider the complexity of real Fog nodes implementation - Unknown attacks are not well addressed
[105]	Distributed network attack detection for IoT systems using Fog nodes and Deep Learning	- Fast detection of attacks - Scalable as the system grows	- Heterogenous IoT may cause compatibility issues - Did not validate real IoT application
[108]	Distributed network attack detection for IoT system using Fog nodes and Deep Learning	- Fast detection of attacks - Scalable as the system grows	- Heterogenous IoT may cause compatibility issues - Dataset used to test the model was not specifically for IoT

Researchers also proposed the application of ML and DL techniques for analysing data related to Smart Cities [23], [24], [25], [14], [21], [87], [50], [66], [116], [65]. Diro & Chilamkurti (2018) proposed using nodes in Fog computing as the distributed network attack detection for IoT systems. Deep Learning is used as the technique to detect malicious network traffic [108]. The approach employs Fog nodes at the IoT level as the main distributed IDS in the IoT environment. One master IDS will coordinate the parameter sharing and optimisation of the trained model for detection using Deep Learning. The authors argued that the sharing system can enable the distributed nodes to obtain a better learning model since the nodes share the best parameters of features from other nodes that can also avoid local overfitting. The approach presented in the paper became one of the common uses of Fog nodes in IDS for IoT systems [117]. However, in the study, the model was tested in a simulated environment with a publicly available NSL-KDD dataset that was not specifically using IoT network packets for normal and attack traffic.

TABLE IV. CYBERSECURITY ISSUES IN SMART CITIES, PROPOSED STANDARDS AND FRAMEWORKS

	Cybersecurity issues and key challenges of Smart Cities	**Proposed standards and frameworks to address the challenges**
[8]	- Attacks on Smart Cities' infrastructure in Software, Network and Sensing layers	Regulations and guideline improvements Government policies for governance and audit Awareness for security risk Secure product developments with built-in security measures tailored to resource constrained IoT devices
[10]	Lack of policies and standards in cybersecurity measures of Smart Cities, technical standards and regulatory framework	Improvement of policies and standards
[12]	IoT adoption readiness for Smart Cities	Understand IoT technology adoption in Smart Cities
[23]	Critical infrastructure security challenges Network security challenges	Implementation of cloud security programs, post-disaster recovery plans, operational security, IoT security risk, user training and application security
[24]	Technical challenges: security and privacy, IoT big data analytics and deep learning limitation Business challenges: planning, cost and quality of service	Development of framework and standards for utilisation of the computing infrastructure used for IoT data analytics, including cloud, fog, and edge computing Use suitable DL technique and dataset for analysis
[25]	Security of data processing layer of Smart Cities Current state of adoption and maturity issues between IoT applications.	Distributed stream processing framework enhancement Data analytic techniques and tools for IoT data processing
[26]	Policies and standardisation issues for Smart Cities related to technology utilisation	Assessment of technical and policy success for Smart Cities application data and services
[13]	Traditional functions of security interventions for an evolved Smart Cities concept	Security interventions in Smart Cities
[15]	Illegal access to information and attacks that cause physical disruptions in service availability	A clear theory of law and rights is needed to define the method of handling security and privacy
[14] [16]	Trust, operational, transitional, and technological Smart Cities interaction framework	Development of Smart Cities security & privacy framework that provides a guideline in the domain of law and regulation, well-being and quality of life, governance, services, mobility, standards and protocols
[37]	Crucial need for methodologies to evaluate the security level of an IoT solution through a checklist that considers the security aspects of the three layers of the IoT architecture	Development of checklist that considers the security aspects of the three layers of the IoT architecture
[18]	Security issues: availability, reliability, mobility, data confidentiality, management of network and its resources, scalability and interoperability, security and privacy, software-defined network, virtualisation and standardisation processes, working ability and performance compatibility with 5G communication	Implementation of precise standardisation, policies and technology implementation
[109]	Network Attack	Network security framework in an IoT environment using a hybrid combination of signature-based and anomaly-based detection methods with the use of the Fog computing architecture.
[116]	Cyber resilience APT and lack of formal methodologies that address the application of digital forensics in incident responses	Utilise automation and AI to control several key functions DFIR using CPS frameworks and systems

D. Proposed Standards and Frameworks to Address Cybersecurity Challenges in Smart Cities

The explosive growth of IoT integration in Smart Cities, as discuss in the previous section, shown the growing threat posed by inherent cybersecurity weaknesses within the underlying technology [25], [38], [98], [114], [118]. Due to the growing adoption of IoT in Smart Cities with Internet access and connection, IoT is now creating cybersecurity threats from malicious entities with unlawful intentions which has become a significant threat to Smart Cities. To answer RQ3 of this study, development and enhancement of policies, standards, protocols and frameworks are suggested as proposed solutions in Table IV above.

E. Combination of Fog Computing and Machine Learning to Address Cybersecurity Challenges in Smart Cities

The literature review in this study promotes the integration of Fog computing with ML and DL for optimal delivery in addressing cybersecurity concerns involving IoT within Smart Cities. Fog computing is instrumental in processing, complemented by ML and DL as analytical techniques for detection and prediction, enhancing the overall efficacy of cybersecurity measures in Smart Cities. A hybrid approach for intrusion detection in IoT systems using Fog computing architecture was published by de Souza et al. (2020).

In this paper, the authors proposed an IDS that covers two steps: binary classification and multi-class classification. The Deep Neural Network (DNN) and k-Nearest Neighbour (KNN) algorithms were implemented as the binary and multi-class classifiers. In the binary classification, the packets were initially checked as either normal or malicious packets, and the malicious packets are forwarded to the multi-class classifier to further classify the types of attack and to check for false positives from the binary classifier. An openly available NSL-KDD dataset that collects normal and attack packets in the network was used to test the proposed model in the paper [20]. This approach was also proposed by other researchers [60]. It provides a good example for fast detection at the binary classification. Further analysis for packets detected as malicious can be done at the multi-class classifier. The same approach was implemented in this research.

NG & Selvakumar (2020) proposed a framework that applies Fog nodes to detect a malicious network as well as a central Fog node to train the AI model [105]. It is a similar approach as the one reported by Diro and Chilamkurti (2018) [108]. However, NG & Selvakumar (2020) used Vector Convolutional Deep Learning (VCDL) for detection and applied the BoT-IoT dataset which specialises in normal and attacked network traffic for the IoT environment. In [105], the authors argued that their proposed framework had performed better than other frameworks previously reported, moreover, their framework was tested using a dataset for IoT networks. However, the framework was not assessed on a real IoT environment. Therefore, similar to [108], the complexity of IoT environment implementation (such as in Smart Cities) may cause issues during framework application.

Pacheco et al. (2020) proposed an IDS framework that uses the Artificial Neural Network (ANN) technique to detect compromised Fog nodes within the IoT environment [114]. The framework has a similar approach as the one reported in [97]. In the approach of [97], the authors applied the Snort software, a commonly used open-source IDS, as the malicious traffic detection, whereas in [114], the framework uses ANN to detect malicious traffic. The dataset for the experimental procedures in [114] was developed by the authors in a simulated IoT testing environment. The proposed framework has good potential for application in IoT implementation for Smart Cities since it detects compromised Fog nodes. However, validation on actual IoT implementation must be performed to determine whether the framework can cope with the complexity of IoT systems in real-world applications.

A comprehensive study on Deep Learning and publicly available datasets was accomplished in [72]. In this paper, a Fog-based attack detection framework for IoT networks was developed, similar to the studies of [20], [22], [46], [105]. In the proposed framework, Deep Learning techniques were used as the detection method. The authors performed experiments using six Deep Learning techniques and five different datasets. Based on the experimental results, the authors concluded that the Long Short-term Memory (LSTM) technique, which is the supervised technique, was the best Deep Learning technique for detecting attacks in IoT networks. The paper served as a good reference for the implementation of Deep Learning techniques as a detection method for IoT network attacks. However, validation in the real implementation of IoT systems can be extended to determine whether Deep Learning techniques can cope with the complexity of IoT communication protocols and customised devices.

The authors in [49] proposed a framework called the intelligent intrusion detection system (I-IDS) to identify attacks in IoT networks. The framework uses Fog nodes as the main detection points in the IoT environment. The authors applied Machine Learning techniques as the detection methods which had concluded that the Markov model was the best technique for detecting and classifying attack types. Compared to previous papers, the authors in [49] have shifted their focus away from Deep Learning to Machine Learning. This change is likely due to less resource requirements and simplified implementation associated with Machine Learning. However, Machine Learning methods may have limitations regarding unknown or zero-day attacks which are more proven with the use of the Deep Learning technique. An IoT-Fog-Cloud model for detecting anomalies in IoT networks was proposed in [110]. The model is quite similar to the framework presented in [49]. However, in [110], the authors only used the improved Naïve Bayes and Principal Components Analysis (PCA) as the detection methods.

IV. CONCLUSION AND FUTURE WORKS

Attacks targeting the IoT system within Smart Cities may lead to cybersecurity incidents, potentially triggering catastrophic consequences, given the ongoing global proliferation of IoT device implementations in Smart Cities. The importance of cybersecurity in Smart Cities becomes exceedingly crucial and closely intertwined with IoT connectivity. The lack of universal standards to be used by the designers or developers of Smart Cities, as previously discussed, poses technological challenges in numerous areas of their development. One critical issue that arises is the risk of cybersecurity threats against the IoT system in Smart Cities due to the absence of dedicated cybersecurity standards and assessment frameworks for IoT implementation. The capability of Smart Cities to uphold cybersecurity within its realm is one of the main factors that will determine how successfully it can achieve its goals to create sustainable, resilient and efficient services for its residents. Any deficiency in its competence in protecting IoT security from threats will endanger the privacy, security and livelihood of the city and increase security impact. Hence, there is an urgent need to address the development of a specialised and comprehensive framework for IoT implementation within Smart Cities, focusing on the context of cybersecurity. This study concludes that real-time threat detection and mitigation, facilitated by the integration of fog computing and an artificial intelligence models based on the real time data from IoT devices, constitutes a noteworthy advancement in fortifying IoT infrastructure against cyberattacks. Additionally, the establishment of a framework to prioritize IoT security and guard against potential cyber threats, while seamlessly integrating all facets of Smart Cities infrastructure, is recommended. This study sets a future research direction, emphasizing the creation of security standards and frameworks for Smart Cities. It necessitates a holistic approach, considering the diverse functionalities, standards and pre-existing frameworks inherent in Smart Cities. By doing so, this specialised framework can offer a robust foundation for the secure and efficient deployment of IoT technology within the complex urban environments of Smart Cities, fostering innovation while safeguarding against potential vulnerabilities and cyberattacks.

Acknowledgement

The authors would like to acknowledge all researchers that involved in this study.

References

[1] A. Sumalee and H. W. Ho, “Smarter and More Connected: Future Intelligent Transportation System,” *Association of Traffic and Safety Sciences Research,* vol. 42, no. 2, pp 67–71, 2018.

[2] A. Kankanhalli, Y. Charalabidis, and S. Mellouli, “IoT and AI for Smart Government: A research agenda,” *Elsevier Government Information Quarterly*, vol. 36, no. 2, pp 304-309, 2019.

[3] J. W. Crampton, “Collect it all: National Security, Big Data and Governance,” *Springer GeoJournal*, vol. 80, no. 4, pp 519–531, 2015.

[4] Cisco, “The Internet of Things: Extend the Cloud to Where the Things Are White Paper”. Available at http//www. cisco. com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf, 2017.

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT Security and Privacy: The case study of a Smart Home,” in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops)*, pp 618–623, 2017.

[6] S. K. Gupta, S. Vanjale, S. Rasal, and M. Vanjale, “Securing IoT Devices in Smart City Environments,” in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp 119–123, 2020.

[7] M. Kalinin, V. Krundyshev, and P. Zegzhda, “Cybersecurity Risk Assessment in Smart City Infrastructures,” *Machines*, vol. 9, no. 4, pp 78, 2021.

[8] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, “Landscape of IoT Security,” *Computer Science Review,* vol. 44, pp 100467, 2022.

[9] D. Swessi and H. Idoudi, “A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures,” *Wireless Personal Communication,* pp 1–36, 2022.

[10] M. Vitunskaite, Y. He, T. Brandstetter, and H. Janicke, “Smart Cities and Cyber Security: Are We There Yet? A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership,” *Computer Security*, vol. 83, pp 313–331, 2019.

[11] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, “A Review of Security Standards and Frameworks for IoT-Based Smart Environments,” *IEEE Access*, vol. 9, pp 121975–121995, 2021.

[12] P. Bellini, P. Nesi, and G. Pantaleo, “IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies,” *Applied Science*, vol. 12, no. 3, pp 1607, 2022.

[13] J. Laufs, H. Borrion, and B. Bradford, “Security and the Smart City: A Systematic Review,” *Sustainable Cities Society*, vol. 55, pp 102023, 2020.

[14] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, “A Comprehensive Study of the IoT Cybersecurity in Smart Cities,” *IEEE Access*, vol. 8, pp 228922–228941, 2020.

[15] A. S. Elmaghraby and M. M. Losavio, “Cyber Security Challenges in Smart Cities: Safety, Security and Privacy,” *Journal of Advance Research*, vol. 5, no. 4, pp 491–497, 2014.

[16] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, “Security, Privacy and Risks within Smart Cities: Literature Review and Development of a Smart City Interaction Framework,” *Information System Frontier*, pp 1–22, 2020.

[17] R. Khatoun and S. Zeadally, “Smart Cities: Concepts, Architectures, Research Opportunities,” *Communications of ACM*, vol. 59, no. 8, pp 46–57, 2016.

[18] A. Khanna and S. Kaur, “Evolution of Internet of Things (IoT) and its Significant Impact in the Field of Precision Agriculture,” *Computers and Electronics Agriculture*, vol. 157, pp 218–231, 2019.

[19] W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” *Computer Networks*, vol. 148, pp 283–294, 2019.

[20] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. dos Santos Vieira, “Hybrid approach to intrusion detection in fog-based IoT environments,” *Computer Networks*, vol. 180, pp 107417, 2020.

[21] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, “Internet of Things: Evolution and technologies from a security perspective,” *Sustainable Cities Society*, vol. 54, pp 101728, 2020.

[22] L. Zhou, H. Guo, and G. Deng, “A Fog Computing Based Approach to DDoS mitigation in IIoT systems,” *Comput. Secur.*, vol. 85, pp 51–62, 2019.

[23] C. Ma, “Smart City and Cyber-security; Technologies Used, Leading Challenges and Future Recommendations,” *Energy Reports*, vol. 7, pp 7999-8012, 2021.

[24] S. Ben Atitallah, M. Driss, W. Boulila, and H. Ben Ghézala, “Leveraging Deep Learning and IoT Big Data Analytics to Support the Smart Cities Development: Review and Future Directions,” *Computer Science Reviews*, vol. 38, pp 100303, 2020.

[25] H. Nasiri, S. Nasehi, and M. Goudarzi, “Evaluation of Distributed Stream Processing Frameworks for IoT Applications in Smart Cities,” *Journal of Big Data*, vol. 6, no. 1, pp 52, 2019.

[26] T. Soyata, H. Habibzadeh, C. Ekenna, B. Nussbaum, and J. Lozano, “Smart City in Crisis: Technology and Policy Concerns,” *Sustainable Cities Society*, vol. 50, pp 101566, 2019.

[27] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[28] M. Mahbub, “Progressive Researches on IoT Security: An exhaustive Analysis from the Perspective Of Protocols, Vulnerabilities, And Preemptive Architectonics,” *Journal Network Computing Application*, pp 102761, 2020.

[29] S. Bhatt and P. R. Ragiri, “Security Trends in Internet of Things: A Survey,” *SN Applied Science*, vol. 3, no. 1, pp. 1–14, 2021.

[30] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya, and M. Conti, “IoT-enabled Smart Lighting Systems for Smart Cities,” in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pp 639–645, 2018.

[31] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya, M. H. Tao, and M. F. Zolkipli, “Scalable Machine Learning-based Intrusion Detection System For IoT-enabled Smart Cities,” *Sustainable Cities Society*, vol. 61, pp 102324, 2020.

[32] C. Toma, A. Alexandru, M. Popa, and A. Zamfiroiu, “IoT Solution for Smart Cities’ Pollution Monitoring and The Security Challenges,” *Sensors*, vol. 19, no. 15, pp 3401, 2019.

[33] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, “The Impact of DoS Attacks onResource-constrained IoT Devices: A Study on the Mirai Attack,” *arXiv Prepr. arXiv2104.09041*, 2021.

[34] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (IoT) forensics: challenges,

approaches, and open issues," *IEEE Communication Survey Tutorials*, vol. 22, no. 2, pp 1191–1221, 2020.

[35] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A Deep Learning-based IoT-oriented Infrastructure for Secure Smart City," *Sustainable Cities Society*, pp102252, 2020.

[36] R. Yugha and S. Chithra, "A Survey on Technologies and Security Protocols: Reference for Future Generation IoT," *Journal Network Computing Application*, pp 102763, 2020.

[37] A. Echeverría, C. Cevallos, I. Ortiz-Garces, and R. O. Andrade, "Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation," *Applied Science*, vol. 11, no. 7, pp 3260, 2021.

[38] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things IoT-based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities," *IEEE Access*, vol. 7, pp 79523–79544, 2019.

[39] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future Of Industrial Communication: Automation Networks in The Era of The Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp 17–27, 2017.

[40] S. Forti, M. Gaglianese, and A. Brogi, "Lightweight Self-organising Distributed Monitoring of Fog Infrastructures," *Future Generation Computing System*, vol. 114, pp 605–618, 2020.

[41] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: an Intelligent Anomaly-based intrusion Detection System for IoT Edge Devices," *IEEE Internet Things Journal*, vol. 7, no. 8, pp 6882–6897, 2020.

[42] D. Miessler, "Securing the Internet of Things: Mapping Attack Surface Areas using the OWASP IoT Top 10," 2018. Available: https://owasp.org/www-project-internet-of-things/

[43] J. Arshad, M. A. Azad, M. M. Abdellatif, M. H. U. Rehman, and K. Salah, "COLIDE: a Collaborative Intrusion Detection Framework for Internet of Things," *IET Networks*, vol. 8, no. 1, pp 3–14, 2018.

[44] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. Abbas, "An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security," *IEEE Internet Things Journal*, vol. 7, pp 10250-10276, 2020.

[45] N. Islam, B. Ray, and F. Pasandideh, "IoT based Smart Farming: Are the lpwan Technologies Suitable for Remote Communication?," in *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp 270–276, 2020.

[46] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "Security Analysis of Network Anomalies Mitigation Schemes in IoT Networks," *IEEE Access*, vol. 8, pp 43355–43374, 2020.

[47] V. Visoottiviseth, P. Sakarin, J. Thongwilai, and T. Choobanjong, "Signature-based and Behavior-based Attack Detection with Machine Learning for Home IoT Devices," *IEEE Region 10 Conference (Tencon)*, 2020, pp 829–834, 2020.

[48] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep Recurrent Neural Network for IoT Intrusion Detection System," *Simulation Model Practice Theory*, vol. 101, pp 102031, 2020.

[49] G. Kalnoor and S. Gowrishankar, "IoT-based Smart Environment using intelligent Intrusion Detection System," *Software Computing*, vol. 25, no. 17, pp 11573–11588, 2021.

[50] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine Learning based Solutions for Security of Internet of Things (IoT): A survey," *Journal Network Computing Application*, pp 102630, 2020.

[51] M. Bach-Nutman, "Understanding The Top 10 OWASP Vulnerabilities," *arXiv Prepr. arXiv2012.09960*, 2020.

[52] P. Ferrara, A. Mandal, A. Cortesi, and F. Spoto, "Static Analysis for the OWASP IoT Top 10 2018," *Proceeding of SPIoT'19*, vol. 19, pp 1-5, 2019.

[53] K. Kimani, V. Oduol, and K. Langat, "Cyber security Challenges for IoT-based Smart Grid Networks," *Int. Journal of Critical Infrastructure Protection*, vol. 25, pp 36–49, 2019.

[54] A. Wani and S. Revathi, "Ransomware Protection in loT using Software Defined Networking," *Int. Journal Electrical and Computer Engineering*, vol. 10, no. 3, pp 3166–3175, 2020.

[55] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture," *Sensors*, vol. 20, no. 16, pp 4372, 2020.

[56] M. Yousif, C. Hewage, and L. Nawaf, "IoT Technologies during and beyond COVID-19: A Comprehensive Review," *Future Internet*, vol. 13, no. 5, pp 105, 2021.

[57] V. Chierzi and F. Mercês, "Evolution of IoT Linux Malware: A MITRE ATT&CK TTP Based Approach," in *2021 APWG Symposium on Electronic Crime Research (eCrime)*, pp 1–11, 2021.

[58] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," in *Digital Twin Technologies and Smart Cities*, Springer, pp 123–149, 2020.

[59] N. N. Thilakarathne and W. D. Madhuka Priyashan, "An Overview of Security and Privacy in Smart Cities," *IoT IoE Driven Smart Cities*, pp 21–44, 2022.

[60] N. Chaabouni, M. Mosbah, A. Zemmari, and C. Sauvignac, "A OneM2M Intrusion Detection and Prevention System based on Edge Machine Learning," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, pp 1–7, 2020.

[61] S. Medileh *et al.*, "A Flexible Encryption Technique for the Internet of Things Environment," *Ad Hoc Networks*, vol. 106, pp 102240, 2020.

[62] J. Fan, W. Yang, and K.-Y. Lam, "Cybersecurity Challenges Of IoT-enabled Smart Cities: A Survey," *arXiv Prepr. arXiv2202.05023*, 2022.

[63] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an Exhaustive Survey on IoT Vulnerabilities and a First Empirical look on Internet-scale IoT exploitations," *IEEE Communication Survey Tutorials*, vol. 21, no. 3, pp 2702–2733, 2019.

[64] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges," *Smart Cities*, vol. 4, no. 2, pp 429–475, 2021.

[65] R. Ahmad and I. Alsmadi, "Machine Learning Approaches to IoT Security: A Systematic Literature Review," *Internet of Things*, pp 100365, 2021.

[66] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp 1686–1721, 2020.

[67] F. Al-Turjman and J. P. Lemayian, "Intelligence, Security, And Vehicular Sensor Networks in Internet of Things (IoT)-enabled Smart-Cities: An Overview," *Computer Electrical Engineering*, vol. 87, pp 106776, 2020.

[68] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT New Features on Security And Privacy: New Threats, Existing Solutions, and Challenges Yet To Be Solved," *IEEE Internet Things Journal*, vol. 6, no. 2, pp 1606–1616, 2018.

[69] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT," *Computer Security*, vol. 78, no. 2, pp 126–142, 2018.

[70] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and Mitigation of Sinkhole Attacks in Wireless Sensor Networks," *J. Computer System Science*, vol. 80, no. 3, pp 644–653, 2014.

[71] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. JPC Rodrigues, and Y. Park, "Designing Efficient Sinkhole Attack Detection Mechanism in Edge-based IoT Deployment," *Sensors*, vol. 20, no. 5, pp 1300, 2020.

[72] A. Samy, H. Yu, and H. Zhang, "Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning," *IEEE Access*, vol. 8, pp 74571–74585, 2020.

[73] W. N. W. Muhamad *et al.*, "Evaluation of blockchain-based data sharing acceptance among intelligence community," *International Journal of Advance Computer Science Application*, vol. 11, pp 597–606, 2020.

[74] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance," *Computer Networks*, vol. 191, pp 108005, 2021.

[75] A. Biryukov and D. Feher, "ReCon: Sybil-resistant Consensus from Reputation," *Pervasive and Mobile Computing*, vol. 61, pp 101109, 2020.

[76] M. Noorafiza, H. Maeda, R. Uda, T. Kinoshita, and M. Shiratori, "Vulnerability Analysis using Network Timestamps in Full Virtualization Virtual Machine," in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, pp 83–89, 2015.

[77] N. M. Noor, N. A. M. Razali, S. N. S. A. Sham, K. K. Ishak, M. Wook, and N. A. Hasbullah, "Decentralised Access Control Framework using Blockchain: Smart Farming Case," *International Journal of Advance Computer Science Application*, vol. 14, no. 5, 2023.

[78] N. Noor, N. Matrazali, N. Malizan, K. Ishak, M. Wook, and N. Hasbullah, "Decentralized Access Control using Blockchain Technology for Application in Smart Farming," *International Journal Advance Computer Science Application*, vol. 13, no. 9, 2022.

[79] W. N. Wan Muhamad *et al.*, "Enhance Multi-factor Authentication Model for Intelligence Community Access to Critical Surveillance Data," 6th International Visual Informatics Conference, pp 560–569, 2019.

[80] N. A. M. Razali, W. N. W. Muhamad, K. K. Ishak, N. J. A. M. Saad, M. Wook, and S. Ramli, "Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities," *IAENG International Journal of Computer Science*, vol. 48, no. 1, pp 18-31, 2021.

[81] CyberSecurity Malaysia, "Secure, Guidelines for (IoT), Internet of Things," Available: https://www.cybersecurity.my/data/content_files/56/2074.pdf.

[82] J. Koo and Y.-G. Kim, "Interoperability Requirements for a Smart City," in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, pp 690–698, 2021.

[83] M. Bauer, L. Sanchez, and J. Song, "IoT-Enabled Smart Cities: Evolution and Outlook," *Sensors*, vol. 21, no. 13, pp 4511, 2021.

[84] B. Mukherjee *et al.*, "Flexible IoT Security Middleware for end-to-end Cloud–Fog Communication," *Future Generation Computer System*, vol. 87, pp 688–703, 2018.

[85] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine Learning And Data Analytics for the IoT," *Neural Computing Application*, pp 1–29, 2020.

[86] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time Big Data Processing for Anomaly Detection: A Survey," *Int. J. Inf. Manage.*, vol. 45, pp 289–307, 2019.

[87] M. A. Amanullah *et al.*, "Deep Learning and Big Data Technologies for IoT Security," *Computer Communications*, vol. 151, pp 495–517, 2020.

[88] P. P. Ray, "A Survey of IoT Cloud Platforms," *Future Computer Informatics Journal*, vol. 1, no. 1–2, pp 35–46, 2016.

[89] R. Arora, S. Gera, and M. Saxena, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp 458–463, 2021.

[90] T. Wu, F. Breitinger, and I. Baggili, "IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp 1–15, 2019.

[91] M. Aazam, S. Zeadally, and K. A. Harras, "Fog Computing Architecture, Evaluation, and future Research Directions," *IEEE Communication Magazine*, vol. 56, no. 5, pp 46–52, 2018.

[92] A. A. Mutlag, M. K. Abd Ghani, N. al Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling Technologies for Fog Computing in Healthcare IoT systems," *Future Generation Computer System*, vol. 90, pp 62–78, 2019.

[93] B. B. Rad and A. A. Shareef, "Fog Computing: A Short Review of Concept and Applications," *IJCSNS Int. J. Computer Science Network Security*, vol. 17, no. 11, pp 68–74, 2017.

[94] S. Kunal, A. Saha, and R. Amin, "An Overview of Cloud ‐ Fog Computing: Architectures, Applications with Security Challenges," *Security Privacy*, vol. 2, no. 4, pp e72, 2019.

[95] T. P. da Silva *et al.*, "Fog Computing Platforms for Smart City Applications-A Survey," *ACM Trans. Internet Technolgy*, vol. 22, issue 4, pp 1-32, 2022.

[96] R. A. C da Silva and N. L. S da Fonseca, "On the Location of Fog Nodes in Fog-Cloud Infrastructures," *Sensors*, vol. 19, no. 11, pp 2445, 2019.

[97] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-things Environments," *Computer Security*, vol. 74, pp 340–354, 2018.

[98] H. Zahmatkesh and F. Al-Turjman, "Fog Computing for Sustainable Smart Cities in the IoT Era: Caching Techniques and Enabling Technologies - an Overview," *Sustainable Cities Society*, vol.59, pp 102139, 2020.

[99] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," *IEEE Communication Survey Tutorials*, vol. 22, no. 4, pp 2489–2520, 2020.

[100] M. De Donno, K. Tange, and N. Dragoni, "Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog," *IEEE Access*, vol. 7, pp 150936–150948, 2019.

[101] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network," *IEEE Access*, vol. 6, pp 73713–73723, 2018.

[102] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog Computing Security and Privacy for the Internet of Thing Applications: State-of-the-art," *Secur. Priv.*, vol. 4, no. 2, pp e145, 2021.

[103] R. Priyadarshini and R. K. Barik, "A Deep Learning-based Intelligent Framework to Mitigate DDoS Attack in Fog Environment," *J. King Saud Univ. Inf. Sci.*, vol 34, issue 3, pp 825-831, 2022.

[104] L. Li, M. Guo, L. Ma, H. Mao, and Q. Guan, "Online Workload Allocation via Fog-fog-cloud Cooperation to Reduce IoT Task Service Delay," *Sensors*, vol. 19, no. 18, pp 3830, 2019.

[105] B. A. NG and S. Selvakumar, "Anomaly Detection Framework for Internet of Things Traffic using Vector Convolutional Deep Learning Approach in Fog Environment," *Futur. Gener. Comput. Syst.*, vol. 113, pp 255–265, 2020.

[106] W. Razouk, D. Sgandurra, and K. Sakurai, "A New Security Middleware Architecture based on Fog Computing and Cloud to Support IoT Constrained Devices," in *Proceedings of the 1st international Conference on Internet of Things and Machine Learning*, pp. 1–8, 2017.

[107] K. H. Abdulkareem *et al.*, "A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues," *IEEE Access*, vol. 7, pp 153123–153140, 2019.

[108] A. A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things," *Future Generation of Computer System*, vol. 82, pp 761–768, 2018.

[109] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "An Anomaly Mitigation Framework for IoT using Fog Computing," *Electronics*, vol. 9, no. 10, pp 1565, 2020.

[110] S. Manimurugan, "IoT-Fog-Cloud Model for Anomaly Detection using Improved Naïve Bayes and Principal Component Analysis," *Journal of Ambient Intelligence Humanized Computing*, pp. 1–10, 2021.

[111] N. A. M. Razali *et al.*, "Opinion Mining for National Security: Techniques, Domain Applications, Challenges and Research Opportunities," *Journal of Big Data*, vol. 8, no. 1, pp 150, 2021.

[112] N. A. M. Razali, N. Shamsaimon, K. K. Ishak, S. Ramli, M. F. M. Amran, and S. Sukardi, "Gap, Techniques and Evaluation: Traffic Flow Prediction using Machine Learning and Deep Learning," *Journal of Big Data*, vol. 8, no. 1, pp 1–25, 2021.

[113] D. Nunez-Agurto, W. Fuertes, L. Marrone, and M. Macas, "Machine Learning-Based Traffic Classification in Software-Defined Networking: A Systematic Literature Review, Challenges, and Future Research Directions," *IAENG International Journal of Computer Science*, vol. 49, no. 4, pp 1002-1015, 2022.

[114] J. Pacheco, V. H. Benitez, L. C. Félix-Herrán, and P. Satam, "Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes," *IEEE Access*, vol. 8, pp 73907–73918, 2020.

[115] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for Smart Cities: A Review of Architectures, Integration Trends And Future Research Directions," *Sustainable Cities Society*, vol. 61, pp 102360, 2020.

[116] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," *Smart Cities*, vol. 3, no. 3, pp 894–927, 2020.

[117] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communication Survey Tutorials*, vol. 21, no. 3, pp 2671–2701, 2019.

[118] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communication Survey Tutorials*, vol. 22(3), pp1646-1685, 2020.