IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-art, Advancement, Challenges and Future Research Directions

Usman Khalil[1], Mueen-Uddin[2], Owais Ahmed Malik[1,3], Saddam Hussain[4]

[1]School of Digital Science, Universiti Brunei Darussalam, Jalan Tungku Link, Gadong BE1410, Brunei Darussalam
[2]College of Computing and IT, University of Doha for Science and Technology, Doha, Qatar
[3]Institute of Applied Data Analytics, Universiti Brunei Darussalam, Jalan Tungku Link, Gadong BE1410, Brunei Darussalam
[4]Department of Information Technology, Hazara University, Mansehra, 21120, KPK, Pakistan

Corresponding author: Usman Khalil (uskhalil@gmail.com) and Saddam Hussain (saddamicup1993@gmail.com)

ABSTRACT The mechanisms based on the distributed environment have become an obvious choice for solutions, while they have not been limited only to a specific domain (i.e., crypto-currency). Rather, it has influenced other industries to develop robust privacy and security solutions, such as smart houses, smart electrical grids, smart agriculture, smart health care, smart transportation, etc. These Cyber-Physical Systems heavily depend on IoT-based smart devices that constitute a networked system of devices dependent on each other for the smooth operation of the overall system. Hence, security and privacy have become an integral part of all the architectural frameworks they operate in. The adoption of these architectures, such as the Internet of Things (IoT), Internet of Cyber-Physical Things (IoCPT), Cyber-Physical Systems (CPSs), and Internet of Everything (IoE), has reinforced the need to develop solutions based on a distributed environment. Distributed ledger technology, i.e., Blockchain, has taken the lead and may support the development of solutions with robust privacy and security. We provide an updated review of authentication mechanisms developed on blockchain technology that enforce decentralized architectures. We discuss the security issues regarding the authentication of these IoT-enabled smart devices. We evaluate and analyze the study of the proposed literature schemes that pose authentication challenges in terms of computational costs, communication overheads, and models applied to attain robustness. Hence, lightweight solutions for managing, maintaining, processing, and storing authentication data of IoT-enabled assets are a must. From an integration perspective, cloud computing has provided strong support. In contrast, decentralized ledger technology, i.e., Blockchain, and lightweight cryptosystems are the areas for much more to explore. Finally, we discuss the future research challenges, which present an improvement standpoint to help address the ambiguities.

INDEX TERMS Ubiquitous Computing, IoT, Authentication, IoT-enabled Smart Device, Smart City, Blockchain, Decentralized Ledger Technology, Cyber-Physical System, Internet of Things, Security,

I. INTRODUCTION

The mechanisms based on the distributed environment have become an obvious choice for solutions, while they have not been limited only to a specific domain (i.e., crypto-currency). For the smart city, it is inevitable to refer to an ubiquitous computing system, as it develops a system where all the connecting devices can communicate with each other through the miner, making it possible to create a device-to-device (D2D) or a machine-to-machine (M2M) network [1]. It requires merging other technologies to make an ubiquitous computing system. There is an exponential growth in the number of smart devices connecting to the internet every day. On the other hand, the internet has become a global arena for connecting these IoT-enabled smart devices. Yet, exponential growth has been observed in the number of connected smart devices.

According to the Cisco Internet Business Solutions Group (IBSG) [1], "IoT is simply the point in time when more things or objects are connected to the internet than people." According to the survey, as shown in Figure 1., the world's population in 2003 was 6.3 billion, while connected devices were only 0.5 billion. The figure was 6.8 billion in 2010, while 12.5 billion devices were connected. In 2015, the population grew to 7.2 billion, while the connected device count was at 25 billion. The survey projected the world's population and connected devices to be approximately 7.6 billion and 50 billion in 2020, respectively. Figure 1. also depicts the ratio of connected devices per person on a year-wise count that shows the immense use of connected smart devices [2], [3].

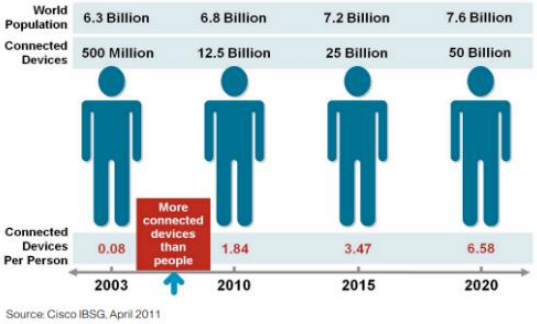

Figure 1. Roadmap of World's Population Vs. Connected devices by 2020 [2]

The survey also depicts the projected year-wise count of connected IoT devices, which shows 15 billion connected devices by 2023, as shown in Figure 2 [3]. Since IoT uses low-powered devices with limited resources in terms of efficiency for data collection, storage, and processing, the architectures have been an open playing ground for attackers. These IoT-related objects and processes have been developed based on the traditional transmission control protocol/Internet protocol (TCP/IP) stack-based internet. They are not designed for such a huge number of connected devices. It requires robust solutions that may provide the foundation for its implementation and integration. Due to the underlying network models, the increasing number of smart

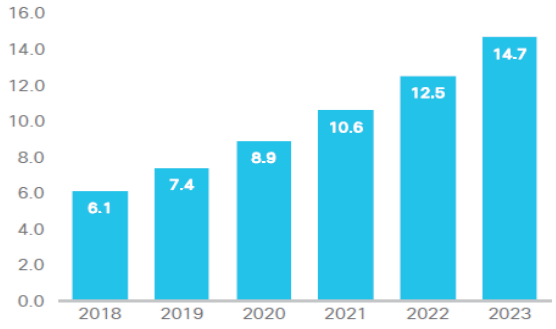

Figure 2. Connected IoT devices by 2023 [1]

devices inherit the issues concerning privacy and security of the connected smart devices and the network itself [4]. These devices play an important role in every domain as they make the edge of the network where real-time data collection is carried out in cyber and physical space. The wide adoption of these smart devices has led to realizing the concept of smart cities, where many smart devices operate in different CPSs. It supported the realization of other cyber-physical systems such as smart houses, smart parking, smart buildings, smart healthcare, etc., as depicted in Figure 4 [5]. Since these devices operate at the edge layer, they are referred to as edge nodes and are typically low-powered and responsible for sending a specific piece of information. The edge nodes work under smart city architecture hence known as IoT-enabled smart devices [6].

II. ENABLING COMMUNICATION TECHNOLOGIES

These smart devices utilize enabling technologies based on the type of network, as depicted in Table 1 [6]. The connectivity provided through these traditional network technologies supports data collection and transfers, as depicted in Figure 4. Since the smart city architecture also relies on the conventional internet supported by communication and transmission technologies for data collection and transmission, respectively, it is evident it may inherit security and privacy challenges. The core of each network is the communication technology through which it communicates. If the medium is not secure or reliable (protocols) enough to provide less resistance for digital signals in the form of the data packet flow, the communication between the devices and data transmission would result in high latency affecting the quality of service (QoS) and security of the network. As discussed in the section above, communication technologies play an important role in connecting devices (i.e., M2M) in an IoT infrastructure; some have been discussed.

As shown in Table 1, the communication technologies have different purposes depending on the range, baud rate, and power consumption [7]. The range differs with respect to technologies from less than 1m to more than 10Kms (i.e., < 1m to >10Kms). As depicted in Table 1, Radio Frequency Identification (RFID), ZigBee, Z-Wave, Bluetooth (BT/LE), Wireless Fidelity (Wi-Fi/HaLow), and Near Field Communication (NFC) transmit the data with low power consumption and hence have been in use by many industries especially the retail and logistics for their business needs. Low-Range Wide Area networks (LPWANs) and Cellular are cloud-based protocols. It operates on the medium access control (MAC) layer and is generally responsible for high data rates over long ranges with medium to high battery power consumption.

With the increase in range, the power consumption increases, which provides a better data rate. It increases as the data rate also differs from 1kbps to 100Mbps depending on the type of services and the power source it uses [6], [7]. Most of these essential technologies have been developed keeping in mind the resource-constrained nature of the IoT-enabled smart devices that eventually supported the

deployment of these smart devices in cyber-physical systems to realize smart city infrastructure.

Table 1
Enabling Communication Technologies

Technology	Range	Baud Rate	Power Consumption
RFID	1m - 2m	1 Kbps	Low
ZigBee	10m - 15m	10 Kbps - 100 Kbps	
Z-Wave			
BLE			
Bluetooth	10m - 15m	1 Mbps	
Wifi	10m - 15m	10 Mbps - 100 Mbps	Medium
Wifi HaLow	10m - 15m	1 Mbps - 10 Mbps	
LPWAN - Licensed			
MYTHINGS	1KM - 2KM	10 Kbps - 100 Kbps	High
LoRa			
SigFox			
LPWAN - Unlicensed			
LTE-M	1KM - 2KM	1 Kbps	High
EC-GSM			
NB-IoT			
Cellular			
5G	1KM - 10KM	1 Mbps - 100 Mbps	High
4G/LTE			
3G			

The use of communication technologies supported data acquisition and transfer using IoT-enabled smart device technologies. The Wireless Sensor Networks (WSNs) and Cloud Computing (CC) have enabled data storage, processing, and analysis in real-time that have made industries save time and amount of expenditure for the maintenance in case of machine break down due to unforeseen events.

A. Wireless Sensor Networks

Wireless Sensor Networks utilize the physical and MAC (Medium Access Control) based on IEEE 802.15.4 standard. It enables the use of LR-WPANs protocols such as 6LoWPAN, CoAP, etc., for WSNs [6]. It is a network of bi-directional sensors wirelessly connected. They are connected so that each sensor senses the environment and sends object-specific data, e.g., location, temperature, humidity, and speed of an IoT device or its surroundings [8]. The collected information is passed to the customer-premises equipment (CPE) for processing. Sensors in WSNs are connected in a multi-hop fashion, allowing multi-hop communication in different network designs for transmitting data from one sensor node to another and then to CPE, as shown in Figure 3 [9]. WSNs operate in different topologies such as Bus Topology, Tree Topology, Star Topology, Ring Topology, Mesh Topology, Circular Topology, and Grid Topology.

Figure 3 further depicts that a sensor node has four main components: the sensing unit, processing unit, transmission unit, and power unit. Every sensor node has a Power Unit powered by the power generator to keep the node alive for collecting data. The node must be powered and active at the time of data collection; otherwise, the data shall be lost (i.e., not in a sleeping state). The collected data is stored and processed by the Processing Unit. The Sensing Unit has a sensor that records the data as specified. The transmission unit transmits and receives the data from the node to the others or CPE via a base station (BS) [6], [10]. As aforementioned, the sensor node collects the object-specified data, and it needs to be alive, which consumes power. That is why the applications and protocols must be developed to prolong the sensor life since the node has an inadequate supply of energy resources (battery power) [10]. WSN is used in different industries such as tracking, navigation, security, maintenance system, etc. For instance, General Electric has used WSN in jet engines, turbines, etc., which analyses the data in real-time, making GE save time and expenditure for maintenance in case engines break down due to overheating [9].

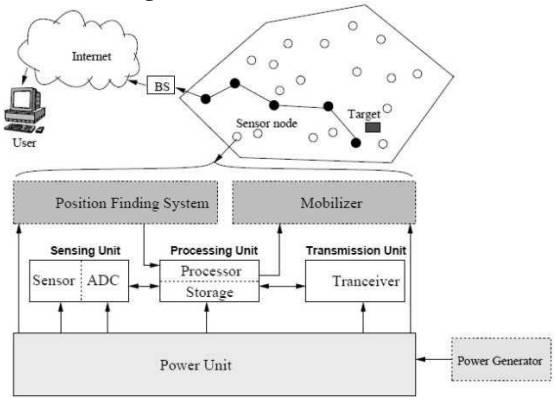

Figure 3. WSNs Scenario with Sensor Node Structure [11]

B. Cloud Computing Concepts

Cloud computing is one major contributor as it provides the framework for smart city infrastructure. It has been defined in three basic levels referred to as tiers for the choice of customers such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) [9]. Cloud computing provides a platform-based service model for data access, storage, analysis, and network to centralized data centers and backbone IP networks. Since smart city infrastructure connects with different cyber-physical systems (CPSs) where devices of different make and models generate heterogeneous data, this data is further processed for analysis and storage in the cloud. By the time the data uploads to the cloud, it loses important information as far as its analysis is concerned, and that's where fog computing takes its place for acting on IoT data and analyzing it to get the useful information out of it [12]. The trend for cloud computing has shifted to fog computing, keeping in view the demands of emerging IoT-based smart city infrastructure.

C. Fog/Edge Computing

Fog computing is one of the latest research trends in regards to computing, storage, control, and networking in which the services are provided to the end-user alongside the cloud [13]. IoT-enabled smart devices within a CPS that generate data are called fog nodes deployed anywhere in the smart city network. For instance, the sensors alongside roads or on the poles, in a vehicle, or on an oilrig are referred to as fog nodes, this also includes the switches, routers, and servers, so any device with computing, storage, and network connectivity can be a fog node [12]. Thus, sending layer in smart city architecture comprises an edge and fog layer. It deploys the edge and fog devices such as sensors, aggregators, actuators, and raspberry Pi/servers to get real-time data processing. Later, the collected data can be used to make informed decisions based on CPS requirements in a smart city, as depicted in Figure 4.

D. Software-Defined Networking (SDN)

Software-defined networking (SDN) technology is another communication approach that enables network management dynamically and efficiently to improve network performance. The software-defined networking is different from the conventional network management techniques as it programmatically improves the network performance and monitoring.

The core concept of SDN is to take out all the control functions from the network devices and merge them in a centralized location. It is one of the drawbacks of SDN from a security and privacy perspective, but it varies with the characteristics of different SDN implementations [14]. It provides the interface more like cloud computing, making it easier to enhance the network management features. On the other hand, it is meant to provide the elasticity for easy troubleshooting as far as the current networks are concerned. This property is important for the smart city infrastructure as scalability and monitoring can be done proficiently. However, the centralization of the intelligence has its drawbacks to scalability and security, which we will explore in this review article compared to distributed architecture [5], [14].

Here, the security of IoT-enabled smart devices in smart cities gets immensely important, specifically from an authentication standpoint. In the case of unauthenticated/malicious assets, the whole infrastructure would be at stake. Many researchers in academia and industries have proposed different methods to secure these smart devices and the data generated by them. Considering these issues, we will be reviewing the literature focusing on authentication mechanisms and the representation of IoT-enabled smart devices in smart cities.

III. Related Surveys

Several surveys discuss the security challenges posed to IoT-enabled smart assets in a smart city context.

The authors discuss the IoT authentication issues in [15], provided with a wide range of authentication protocols proposed in the literature. Using a multi-criteria classification, they compare and evaluate the proposed authentication protocols, showing their strengths and weaknesses in multiple CPSs. They identify several requirements and open issues that may be considered while developing new authentication schemes for IoT networks and applications. The authors in [16] identify several key technical challenges and requirements for the IoT communication systems based on privacy, security, intelligent sensors/actuators design, low cost and complexity, universal antenna design, and friendly smart cyber-physical system design for its deployment. Finally, the authors present challenges in cyber-physical communication system deployment and related issues in implementing an efficient and effective IoT communication system.

A comprehensive survey has been presented in [17] on cyber-physical systems (CPSs) concerning applications, technologies, standards, and related security vulnerabilities, threats, and attacks. It further leads to identifying the key issues and challenges within this domain. Additionally, the existing security measures have been discussed and evaluated to strengthen the identification of limitations further. Various security aspects, services, and best practices ensure resilient and secure CPS systems. The survey focuses on the CPSs that face challenges regarding security services, authentication, and authorization with suggestions and recommendations.

The review in [3] presents the overview of layered architectures of IoT and attacks associated with it. The mechanisms that provide the security solution to the security issues have been discussed, with the limitations posed in the same direction. The survey reviews the existing security mechanisms for protecting the IoT infrastructure and the restrictions and regulations of the current security methods. Several open research challenges associated with IoT technology have also been discussed for better understanding. The literature survey in [18] identifies the components of the smart city to realize the concept. The real-world implementations and statistical analysis are discussed, keeping in view the smart cities context. Since smart cities face serious challenges and issues due to enormous data processing demands and heterogeneity of smart assets, a review of those future research challenges has been identified, describing the opportunities for improvements.

The authors in [19] present current challenges of IoT and Blockchain while an analysis of the potential advantages of both has been evaluated. The review of the available blockchain platforms and disruptive applications in this area has been highlighted to address these challenges. The authors in [20] discuss the characteristics of blockchain technology, focusing on the integration of distributed ledger technology in smart cities. A blockchain-based conceptual architecture explains security using a possible use case study. Also, a real-world blockchain-based smart city case study discussed several imperative research challenges.

The review of the related surveys aforementioned is expanded to multiple domains. However, IoT-enabled smart

devices have become an important part of the architectures, such as the Internet of Things (IoT), Cyber-Physical Systems (CPSs), Internet of Cyber-Physical Things (IoCPTs), and Internet of Everything (IoE). In contrast, these architectures together constitute a system to realize the concept of smart cities and, ultimately, a smart planet. The literature has been reviewed, keeping in view all the architectural domains aforementioned. Security services (CIA), including authentication and authorization (AAA), are of utmost importance to safeguard these smart assets. However, we have taken the lead in providing an updated review of the authentication mechanisms and device identification in a smart city architecture lacking in most of the reviews. This literature review is a continuation work of a comprehensive review article that discussed the newly proposed solutions based on centralized and distributed blockchain-based solutions for authentication of IoT-enabled smart devices. In this article, however, a descriptive approach has been adopted to explore decentralized architectures and discuss the security issues in the authentication of these IoT-enabled smart devices. The review of the proposed schemes has been evaluated based on the robustness and weakness standpoints which will eventually help address the ambiguities for improvement in the future. However, the authentication schemes based on decentralized architectures provoke new challenges. The major contributions of the article are presented below.

- We explore and discuss smart city layered architectures for employing authentication schemes in various smart city scenarios.
- We review and analyze the proposed security services and their related challenges and issues in smart cities.
- We present a comprehensive classification and detailed reviews of the latest authentication schemes for IoT-enabled smart assets in smart cities.
- Furthermore, we categorically reviewed, evaluated, and analyzed IoT-enabled authentication schemes based on decentralized blockchain-enabled smart city architectures.
- We identified and discussed the pros and cons of existing authentication schemes in smart city architectures.
- Finally, we provide the recent advances and future recommendations for IoT-enabled authentication schemes in smart cities and conclude the paper in the final section.

E. Paper Organization

The rest of the paper is organized as follows. Section II discusses the enabling communication technologies for IoT-enabled smart devices in smart cities, followed by Section III presents related literature reviews. Section IV presents the layered architecture of a smart city, while Section V discusses the layered adversaries on each smart city layer. Section VI elaborates on the smart city layered security issues, followed by Section VII, which presents authentication architectures based on blockchain in a smart city. Later on, recent advancements are presented about blockchain-based cryptosystem solutions with future research challenges in Section VIII. Finally, a concise conclusion is presented at the end.

IV. Smart City Layered Architecture

The smart city architecture can be classified into layers based on the assets operating in a physical environment within cyberspace that provides its connectivity with the network for data flow, such as the internet. The data captured by the physical assets, i.e., sensors, aggregators, and actuators, are processed in the physical layer referred to as the sensing layer. The command and control work on the application layer defines the applications for the asset's behavior at the physical layer. The network provides connectivity using communication and transmission technologies at the transmission layer. Though different researchers have different opinions [21], smart city architecture can mainly be divided into three-layered architecture, as depicted in Figure 4. The layers' functions, issues, and weaknesses are further explored and discussed below in this section.

A. Application Layer

The application layer plays an important role in the applications defined with different functions for respective CPSs, such as application deployment for smart homes, smart hospitals, or smart cars. As depicted in Figure 4, this layer provides a path for the interaction using received information from the transmission layer. It executes commands based on data received from the devices at the sensing layer [3], [22]. The deployment is carried out in the security operations center (SOC) in a smart city concept. It is the center point for service providers in a smart city architecture for utility companies connected to several applications located at different locations. The automated services provided at this layer may be centralized or distributed depending upon the nature and requirement of the CPS for its application and scalability.

B. Transmission Layer

As shown in Figure 4, the data from the application layer is transmitted through this layer. It is responsible for the communication among the devices between the upper and lower layers. These devices connect through the traditional network technologies already in use for transferring the collected data, i.e., Wireless Fidelity (Wi-Fi), Radio Frequency Identification (RFID), Bluetooth (BT), Near Field Communication (NFC), etc. In contrast, the transmission technologies such as 3G, 4G, LTE, 5G, internet, or satellite play an important role in data transfer and acts as the backbone for communication [6]. Routing devices such as routers and switches use communication and transmission technologies to route the data. In contrast, cloud computing platforms, internet gateways, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS)

platforms facilitate smooth and secure data transmission. The datacenters by web servers such as Facebook, Google, etc., also function at this layer which may be centralized or decentralized in nature, as in the case of Interplanetary File System (IPFS), Swarm, or S3, etc.

C. Sensing Layer

Next to the transmission layer is the sensing layer. It comprises an edge and fog layer and deploys the edge and fog devices such as sensors, aggregators, actuators, and raspberry Pi/servers, respectively, to get the real-time data processing. Later, the collected data can be used to make informed decisions based on CPS requirements in a smart city, as depicted in Figure 4. For instance, actuating the lights to switch on/off, recording a video whenever any moving object is detected, or turning on/off any smart device whenever sensing the heat signatures triggers environment sensing that can be used to intimate the SOC for further action, etc.

V. Smart City Layered Adversaries

The smart city concept can improve the efficiency of the maintenance and replacement operations of the involved devices, keeping adversaries in view. The data transfer among the layer and devices is of utmost importance as data integrity, and anonymity preserves the data being leaked. In contrast, user and device authentication prevents unauthorized access in case of an attack vector. In this section, the smart city pyramid has been shown and is further explored from an adversarial point of view, as discussed below and depicted in Figure 4.

A. Application Layer Adversaries

Since the user interaction is provided through the application layer, the attack vector finds it lucrative to exploit loopholes that are left unattended consciously or for a better end-user experience. The most common attacks at this layer are injection attacks [23]–[25], cross-site scripting attacks[3], [26], [27], parameter tampering [28], [29], botnet attacks, and buffer overflow attacks [30], [31].

A. Transmission Layer Adversaries

This layer can be targeted by obstructing the network resources and bombarding the fake data. It can lead to serious consequences such as distributed denial of service attacks (DDoS). The other types of attacks may be similar attacks, i.e., trojan attacks [32]–[34], worm attacks [17], [35], [36], Denial-of-Service attacks (DoS) [3], [19], [34], [37], or data can be spoofed by Man-in-the-middle attacks (MITM) [3], [4], Meet-in-the-middle attacks (MeetITM) [38], and repudiation attacks [39] while one-way encryption schemes are best suited to hinder the attack vector [30], [40]–[42].

A. Sensing Layer Adversaries

The devices at the edge have to be protected in case of attacks, or the assets may be damaged or stolen. As discussed below, the adversaries at the sensing layer, such as physical attacks [3], [24], port scanning attacks [4], eavesdropping [43], [44], and replay attacks [3], [17], are the most common attack for data spoofing and checking the behavior of the environment in which they operate [43], [45]–[47].

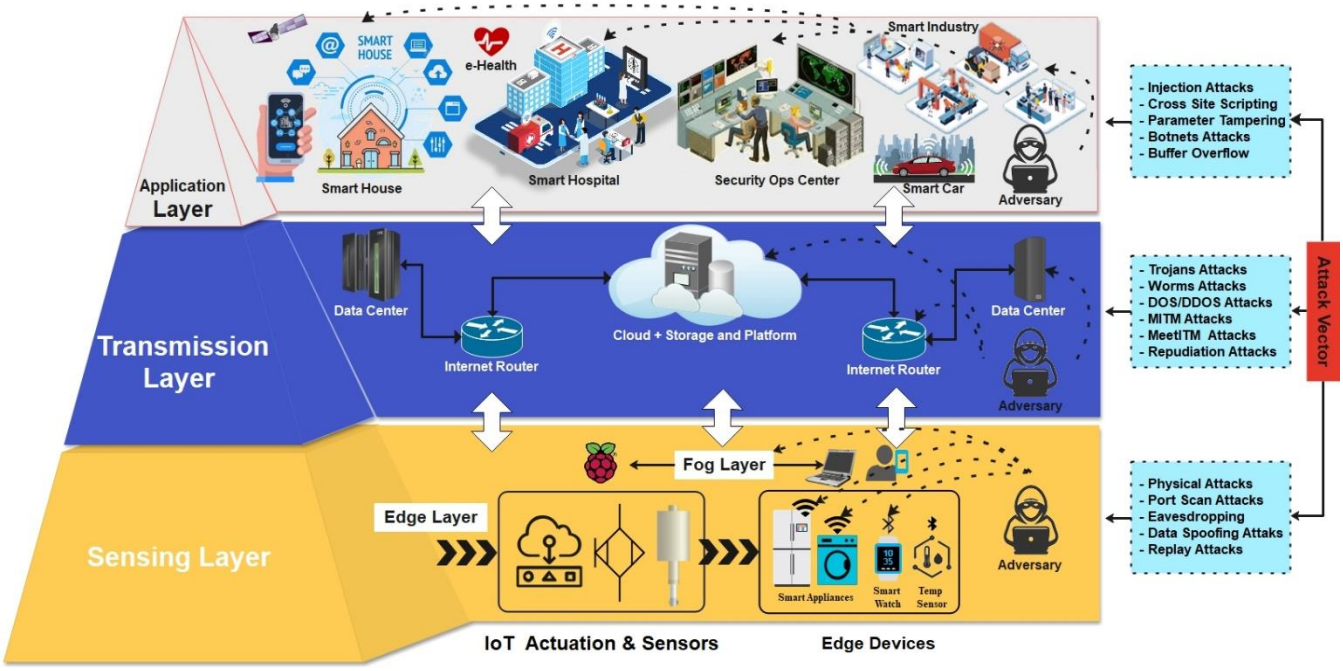

Figure 4. Generalized Smart City Layered Architecture

VI. Smart City Layered Security Issues

Though the internet provides a platform for connectivity and makes an ecosystem where all the assets will communicate (D2D, M2M, etc.), it is unsafe. Many specialists and researchers believe that "IoT is going to hit us hard if we're not doing anything about it." [48]. For every service, every process, an API, the attack vector would always be looking to find the loopholes to break through the various layers of security mechanisms and protocols. A review of security issues keeping in view the same has been discussed in this section, leading to the current evaluation of security issues in smart city infrastructure.

A. Security Issues in Internet Infrastructures

As stated in Section I, the use of IoT-enabled smart devices is not limited to any specific field or industry. The objects associated with them have become more intelligent and smarter. These devices are prone to security issues exploited by the attack vectors on different communication layers. These attacks have been categorized as physical attacks, physical and link-layer attacks, sensing layer attacks, network layer attacks, application-layer attacks, and multilayered attacks [5]. If compromised, these smart devices become the mainstream arena for cyberattacks to exploit the vulnerabilities of the devices and deploy IoT botnet attacks that cause major issues in the internet core for data transmission.

An example, in this case, is MIRAI BOTNET. The group utilized "Mirai" to scan the internet and found the IoT-enabled smart devices vulnerable to a cyberattack with their default login details. The assets were hacked and were used to attack a huge botnet that chocked half of the internet in the United States and was named "the most serious distributed denial-of-service (DDoS) attack in the history of the country [49]. Attacks like DoS and DDoS jammed the network flow [30], while the increasing number of IoT networks have faced challenges based on the security and privacy of the smart devices and data generated [50].

B. Security Issues in Cyber-Physical Systems

Security is a critical requirement for building IoT-enabled smart devices in a smart city, as this includes both secure communication and strong authentication for users and devices. In context to CPSs such as fields of smart grid, health monitoring, smart vehicles (UAVs, UGVs), process control, oil, and gas distribution, transportation system, etc., more complex large-scale systems have been developed and deployed at the industry level, such as Supervisory Control and Data Acquisition system (SCADA) [51], [52]. These CPSs provide command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities, considered the backbone of any industrial architecture [52].

C. Security Issues in Industrial Cyber-Physical System

As detailed earlier, the customer premises equipment (CPE) in cyber-physical systems (CPSs) generates data (sensors) which is crucial to making informed decisions (actuators) or decisions for corrective measures to resolve operational issues. In contrast, implementing these devices in a corporate system like Supervisory control and data acquisition (SCADA) is critical. Here the authentication becomes of immense importance from an adversarial point of view that may cause serious damage to the CPS, as in the case of the industrial programmable logic controllers (PLCs). The automated engagement of electromechanical processes for controlling the machines and industrial processes such as separating nuclear material from the centrifuges is performed. In case of a data breach, wrong data fueling may cause serious damage to the overall system or, in worst-case scenarios, be destroyed, causing a system halt [52]. A similar kind of security breach was reported in 2007. The Iranian Nuclear Program was hit by the Stuxnet virus, which works by propagating information across the network and the USB sticks [36]. The virus compromised Iranian PLCs, collecting data on industrial systems, and caused the fast-spinning centrifuges to tear themselves apart [52]. According to Reuters, an asset protection US-based company, "Target," was breached via the network to access the embedded devices with impunity. It caused a serious security risk to the data breach that hit 40 million payment cards data breach in the year 2013 [53]. The cyber-attack on the German steel plant in 2014 caused significant damage where the attack vector accessed the corporate network and moved unilaterally throughout the control network or operation network without any operational defenses in place [54].

D. Security Issues in Health Care

In the case of the healthcare CPS, the issues related to the weak security in the wireless embedded medical devices such as pacemakers and insulin pumps (which record the patient details and treat the respective patients accordingly) may leak the patient's critical health information. In case of false data injection, the results may be fatal. There had been major adversaries in the past where the vulnerabilities in the smart assets were exploited. A report was released on Dec. 29, 2016, by the US Food and Drug Administration (FDA) about the smart devices currently available in the market. It mentioned the issues related to the network security in the wireless embedded medical devices such as pacemakers and insulin pumps, which could leak the patient's critical health information [4], [55]. Here, the authentication of connected devices has to be ensured while sending data to the corresponding storage devices, which is critical as far as the patient is concerned [4], [50], [55].

E. Security Issues in IoT-enabled Smart Devices

Another factor is the manufacturers' low concentration of security features in the CPE, such as easy to guess default login credentials, open ports, unencrypted and weak versions of SSL (v2, v3, and CBC mode) services, self-signed or expired security certificates, etc. Thus, it becomes an easy target for the attack vector that exploits these features to attack the system as a botnet. It happened a couple of times in the past. The manufacturers of these devices left unattended authentication and access control schemes which increases the chance of exploitation by the attack vectors.

In [30], an analysis of the ten most popular consumer IoT devices showed 250 susceptibilities concerning outdated operating systems, open telnet ports for making a remote connection to the device for exploitation, and weak encryption protocols configuration for data transmission. Authors in [31] evaluated 45 IoT devices from well-known vendors such as Amazon (Echo, Fire TV), Apple (HomePod, TV), D-Link (Cloud Camera), Google (Home, Home Mini, OnHub), Philips (HUE), TP-Link (Wi-Fi Bulb, Wi-Fi Plug), Samsung (Smart Things, Smart TV) and Logitech (Harmony), etc. They found almost the same kind of issues together with 84 running services. Secure Shell (SSH), Universal Plug n Play (UPnP), HyperText Transfer Protocol (HTTP webserver), Domain Name System (DNS), Network Virtual Terminal Protocol (Telnet: A service for remote connection to devices), Real-Time Streaming Protocol (RTSP) and custom services to name a few, while 39 issues related to those services were found. Though there have been many state-of-the-art authentication and authorization mechanisms that have been proposed for devices in smart cities, most of them are centralized and offer high communication overhead, which results in higher energy consumption.

1) Security Issues in Heterogeneous IoT-enabled Smart Devices

Different manufacturers and vendors produce IoT-enabled smart devices that use various security and communication protocols to connect to the same IoT infrastructure. Since these heterogeneous devices connect in the same CPSs, it makes a heterogeneous infrastructure for data transfer and communication mechanisms at respective layers. It also makes the infrastructure generate a huge amount of heterogeneous data. The authors in [5] also discuss the IoT infrastructure regarding the heterogeneous data generated by the heterogeneous things (IoT devices). The collection of this data poses an open challenge because of its volume and nature. It is important to take care of this data as hackers can easily hack it from IoT assets and later use it to manipulate the devices, such as Botnet attacks.

VII. IoT Enabled Smart Devices Authentication Architectures in Smart Cities

As discussed earlier, the issues in a smart city can also be put into fundamental security traits categories, i.e., Authentication, Authorization, and Audit (AAA), which further classifies the security services into Confidentiality, Integrity, and Availability (CIA). In contrast, user confidentiality and authentication aspects have been explored. For any CPS in smart city infrastructure, the authenticity of users and customer premises equipment (CPE), i.e., sensors and actuators, are major concerns. With the rapid increase in usage and low concentration on the security and privacy details of the devices, challenges have been evident, pushing the need for solutions that could address these security issues.

Since this paper focuses on IoT-enabled smart device authentication schemes in a smart city, the upcoming section discusses the review of traditional state-of-the-art authentication mechanisms already deployed, followed by the newly proposed authentication mechanisms. A categorical approach has been opted to discuss an up-to-date survey of the conventional and freshly proposed authentication schemes based on centralized and decentralized architectures.

A. IoT Authentication Schemes based on Distributed Architectures in Smart Cities

A non-centralized system, also known as a distributed system, consists of hosts interconnected by a network. The hosts here refer to the computers in an interconnected computer network. These hosts communicate with each other and other resources in the network, such as files and printers, with the help of network services provided by servers. These resources are shared over the interconnected network and can be used by distributed authorization system [56]. The authorization of the services runs for every software that needs it, which means a copy of authorization and authentication results is saved by the resources locally. Every request acts as a local server, which requires no communication on the network layer [57]. The occasional synchronization with the central service makes it possible to have the updated decision (authorization and authentication decisions) at the edge nodes. It authenticates the hosts at the local level, contrary to the non-distributed system in which every decision request has to go to a centralized server machine for approval, thus making it a centralized system. This attribute of the distributed system poses security problems that are intricate and must be addressed in order to keep the system safe from any sort attack vector. There are multiple reasons of having a distributed system i.e. implementing authentication schemes on different hosts/nodes for IoT devices authentication in a smart city context and that is the reason the system is vulnerable to a variety of adversaries in the form of intruders as well as authentic users of the system. The specific trust assumption has to be studied and evaluated carefully to determine whether the use of a blockchain provides additional value. A review of such proposed authentication schemes for IoT assets has been provided with an analysis of security issues posed by these mechanisms for future research goals.

1) Smart Houses

A case study for a blockchain-based smart home framework that deploys the IoT security model compared to a cloud-based smart home has been proposed [50]. The performance evaluation in terms of fundamental security traits such as confidentiality, integrity, and availability has been performed. The authors define the IoT infrastructure with various components for a smart home using the lightweight blockchain concept for security and privacy issues and discuss the implementation of various transactions and associated procedures. In a smart home, all IoT devices are connected to a miner connected to Blockchain, and a local storage device for storing the data from IoT devices has been introduced. The concept discusses how the Blockchain public key authenticates the network traffic and provides security against DDoS and Link Attacks. The experiment showed that Blockchain is a comparatively more reliable solution for a smart home-based IoT infrastructure regarding security and privacy. At the same time, it proved to be quite manageable for low-energy devices.

The authors analyze the limitations of existing centralized approaches in [58] and propose a blockchain-enabled solution. The proposed solution can trace every operation on the chain, easily verify device and user identity, and set up multiple-level access control to help build a secure smart home system. The authors demonstrate the design architecture and implementation methods as proof of concept.

A blockchain-based smart home framework that deploys the IoT-enabled smart devices security has been proposed [59]. The performance has been evaluated in terms of fundamental security traits such as confidentiality, integrity, and availability. The solution has been designed to overcome reported security limitations in commonly used permissioned Blockchain approaches. The authors proposed architecture containing four layers: Cloud storage, Hyperledger fabric, Hyperledger composer, and a smart home layer. Mapping the attributes of smart home devices to those from the Hyperledger composer has been adopted. It allows for a customized, designed-for-purpose solution that meets IoT-based smart homes' security requirements. The proposed architecture was implemented and tested to improve the authorization and privacy of smart homes and some inherited features, including transparency and interoperability.

2) Blockchain-based Federated Mechanisms

The authors in [60] propose a novel solution for distributed management of identity and authorization policies by leveraging blockchain technology to hold a global view of the security policies within the system and integrate it into the FIWARE platform. The authors aim to use the Blockchain merely as a distributed data repository, leaving the decentralized OAuth2-based implementation of the authentication and authorization logic external to the Blockchain, as provided by FIWARE. It offers a rich set of open standard APIs to acquire data from the IoT of the smart city, process, store such data, and provide advanced user interaction. When such centralized management of policies is not suitable due to the federated deployment applied to the system of interest or the multi-tenant model, more advanced solutions are needed, such as a federation of databases. The performance assessment was achieved via Blockchain using a federation of relational databases by employing a 3PC for guaranteeing consistency among multiple replicas. The mean latency of over 20 requests has been equal to about 390ms with blockchain usage, while it was observed at 700ms using a federated set of databases. The insert/update operations with the blockchain use were measured with 3160ms and 2870ms, respectively, and 50ms and 30ms using a federated database system. The results showed Blockchain as a more beneficial technology when queried rather than implied for data management. The federated database system is faster as the distributed consensus is not needed.

3) Blockchain-based Mechanism

An Ethereum-based smart contract for edge computing has been proposed as SmartEdge in [61] for its low-cost, low-overhead tool for compute-resource management. The authors show the design breakdown of a smart contract into three key steps and describe them below in the context of their design of SmartEdge. Firstly, identify the parties involved in the smart contract, such as compute node (host the Ethereum emulator and the smart contract). Secondly, the data node will be responsible for sending/receiving data as defined in the smart contract, such as identifying key states in the lifetime of the smart contract. Thirdly, the five states are Unavailable, Available, Pending, Computing, Completed and identifying and defining the methods that trigger state transitions. The performance was evaluated in terms of low-overhead delay in executing a job and transaction cost in terms of costs that should not be significant relative to their value. Two factorization jobs were created to evaluate the overhead with input files consisting of 10,000 integers and 100,000 integers using the data node, compute node, and SmartEdge. This job roughly executes in 3 minutes on a Raspberry Pi 3; however, when the job was executed using SmartEdge, it only took 8.6 seconds. There is an overhead of 2 seconds compared to executing the job directly on the compute node. There was a noticeable 2-second overhead that included the time it takes to transfer the job to the compute node and the result back to the data node. The execution time of the larger input file was noted as 67 seconds on compute node, which shows increased latency in terms of larger input files which may affect the time for Available and Completed states.

A blockchain-based decentralized network trust and IoT authentication protocol under the public key encryption system has been proposed [62]. The authors developed the Web of Things (WoT) model that leverages web technologies to improve interoperability and transparency and reduce the chain of trust. A scalable, decentralized IoT-centric PKI has been proposed by combining it with the web-3 authentication and authorization framework for IoT-enabled smart devices. The authors in [63] proposed

authentication and access control mechanisms based on a distributed architecture for lightweight IoT devices, which they claim, can imply many scenarios. The mechanism leverages the benefits of fog computing and public blockchain technologies, which provide a non-centralized medium since public Blockchain is a non-centralized distributed ledger technology. The mechanism provides an initialization phase for registering a new IoT system and a device authentication phase for registering smart devices with blockchain fog nodes. The proposed mechanism provides a D2D communication phase for device communication within or for other systems and access control for IoT devices. The Elliptic Curve Digital Signature Algorithm (ECDSA) has been used for key generation, generating public and private keys for the devices and the fog nodes. The security requirements have been tested with the proposed mechanism: Confidentiality, Integrity, Identification, Non-Repudiation, Authentication, and Mutual Authentication. The evaluation was carried out in terms of execution time required by the IoT node for making the registration request (min: 1.06ms and max: 1.25ms) and the time needed by the node for sending a data message (min: 0.03ms and max: 0.08ms). Also, in terms of the CPU power consumed by the node for requesting registration (min: 7.24mW and max: 10.32mW) and power utilized by the node for sending a data message (min: 2.91 mW and max: 4.12mW). A total of 100 experiments were carried out to evaluate the proposed mechanism, which shows promising results comparatively.

A proposed framework in [64] BCoT Sentry (Blockchain of Things Sentry) integrates Blockchain with an IoT network. It enhances network security by analyzing network traffic flow patterns of the device obtained from data storage in the Blockchain. The framework has been proposed to keep the lightweight feature of IoT devices which commonly fails to meet computationally intensive requirements for blockchain-based security models. (BCoT) Gateways are blockchain nodes where an IoT device security module is employed through a smart contract. These Gateways facilitate recording authentication transactions in a blockchain network; thus, the mechanism stores the device identity information in a distributed ledger. The authors present a novel approach to the feature selection method (similar feature selection method in machine learning utilizing the maximum information coefficient (MIC) used to measure the discrimination of IoT devices). It captures the IoT device network traffic from the network layer and sends this traffic flow feature to the Smart Contract via blockchain transaction. The smart contract defines the device's identity information and related operations and is triggered once the transactions in the Blockchain are posted. The contract defines the access permissions policies that enforce the authorized access to modify or access the device identity information through a defined contract in the web3.py interface. The evaluation performance was measured in terms of device identification accuracy of detecting device identity fraud that exceeds 80%, and 21 of which exceed 90%. In terms of time complexity, 1000 calls were made to the functions *Register ()* and *Detective ()* on each BCoT Gateway and obtained the average response time. The identity authentication for the two parts of the proposed IoT authentication model, Register and Fraud Detection, has a time complexity of O ($m * n$) and O(m), considering the type of IoT device is 'n.' At the same time, there are 'm' IoT devices.

A blockchain-based decentralized authentication modeling scheme named BlockAuth has been proposed in [65]. The edge devices in the edge layer have been regarded as a node to form a blockchain network. The authentication scheme claims are suitable for password-based, certificate-based, biotechnology-based, and token-based authentication for high-level security requirement systems in Edge and IoT environments. A blockchain-based decentralized authentication protocol has been developed using the Blockchain's consensus and smart contract capability. In contrast, a client-server-based approach has been adopted to deploy Blockchain on the server machine. The registration and certificate issuing servers have been deployed for user authentication and access control based on the certificate-based mechanism. BlockAuth Scheme was evaluated by the authentication time required to initiate the request to receive the result. The response time was tested for the centralized network and 4-peer, 6-peer, and 8-peer in the decentralized network. The average response time of 4-peer, 6-peer, and 8-peer in two groups test for the passing scene was recorded as 2.24s, 2.31s, and 2.40s, respectively, and for the failed scene was recorded as 2.22s, 2.30s, and 2.40s, respectively. Comparatively, the average response time of the centralized authentication scheme is noted at 1.13s, which has been significantly lower than the proposed scheme in terms of latency. It might be due to the network speed and consensus mechanism involved in the blockchain scenario. The authentication schemes have been deployed using the smart contracts, while claims for the biotechnology-based and token-based password authentication mechanisms have not been seen. PKI-based implementation in a client-server environment is prone to a single point of failure.

SSO (Single Sign-On) is a one-time password authentication scheme that requires a user to authenticate once, which helps avoid the fatigue of adding passwords again and again on the web. It includes a centralized approach with an authorized central body, such as a miner or server, which registers and issues a token for future access to various services and applications [66]. Alternate to SSO, the authors in [67] proposed a new Distributed Anonymous Multi-Factor Authentication (DAMFA) scheme that uses public Blockchain (i.e., Bitcoin & Namecoin) and the underlying consensus mechanism to improve usability. It is built on a Threshold Oblivious Pseudorandom Function (TOPRF) for resistance to offline attacks. They claim to include a distributed transaction ledger technology such as Blockchain to improve usability. It requires no interaction with the identity provider and hence the user's authentication no longer depends on a trusted third party. Namecoin

blockchain is a public ledger blockchain that allows registering names and stores related values in the Blockchain, a secure distributed shared database. The performance evaluation of the decentralized anonymous authentication system has been carried out in two main steps: the registration phase and the authentication phase. The total time consumed in the registration phase for generating the credentials was noted at ≈ 703ms, while the time consumed in the authentication phase for generating the credentials was noted at ≈ 640ms. The results were achieved by running over 100trials for the authentication and the registration phases.

A framework for the authentication mechanism based on Blockchain has been proposed in [68] named BCTrust. It has been designed especially for devices with resource constraints such as computational, storage, and energy consumption constraints. Public blockchain Ethereum has been used together with C programming to deploy the mechanism to implement the framework. The robustness claimed by the authors is because of the underlying framework of the public Blockchain, which is distributed ledger technology with no central authority for the signing of the contracts and principles known as smart contracts. These smart contracts provide access control over authentication mechanisms for system (SID) and User or Device identification (UID). A practical implementation has been carried out on a network composed of two CPANs. At the same time, the performance evaluation of the proposed mechanism was measured in terms of execution time and power consumption of classical association and BCTrust association. The average time and power consumption of the BCTrust association were noted ≈ at 14,406ms and ≈ 0,681 Joule. In contrast, a Classical association was noted ≈ at 34,450ms and ≈ 2,755 Joule. It shows that BCTrust was more robust in terms of saving more than 75.28 % of energy comparatively.

Blockchain-enabled fog nodes for user authentication schemes have been proposed in [66], which deploy smart contracts to authenticate users to access IoT devices. It is also used to maintain, register, and manage IoT devices, fog nodes, admins, and end-users. The fog nodes provide scalability to the system by relieving the IoT devices from carrying out heavy computation involving tasks related to authentication and communicating with the public Blockchain. A distributed system based on the public blockchain design has been proposed with its implementation using Ethereum smart contracts for IoT devices authentication at scale. The proposed Ethereum smart contract implements the authentication functionality for adding end-users and IoT assets with the help of an Admin who takes care of the overall functionalities and operations of the authentication mechanism.

As aforementioned, the blockchain-based authentication schemes review the distributed ledger technology (DLT) for IoT-enabled smart device authentication in a decentralized architecture; however, these schemes pose threats that the attack vector in cyberspace can exploit. Table 2 depicts an evaluation summary of these proposed authentication schemes. Most proposed mechanisms have been deployed on the Ethereum platform, utilizing the traditional Proof of Work (PoW) consensus mechanism. Ethereum undoubtedly is a platform that supports public, private, and hybrid blockchains to be developed and deployed; also, it provides the option to utilize decentralized applications (dApps) to provide logic to execute the functions as required. However, the consensus mechanism poses performance issues of fault tolerance, decentralization, stability, and high-level security. Other platforms, such as Hyperledger Besu [71], Hyperledger Fabric [72], Solana [73], etc., must be explored for developing solutions over smart contracts. These platforms support more energy-efficient and low latent consensus mechanisms such as IBFT, IBFT 2.0, and Clique, which must be employed for the authentication of IoT-enabled smart devices to support the smart city infrastructure. The issues with those schemes have also been evaluated based on the security services for collaborative authentication, strong fault tolerance, decentralization, stability, and high-level security, which depicts most of the issues relating to access control and data anonymity. These recently proposed mechanisms employ blockchain to attain decentralization

Table 2.
Enabling Communication Technologies

Proposed Mechanism	Blockchain Platform	Ref	Consensus Mechanism	M/ Auth	Access Control	Data Integrity	Data Anonymity	Security & Reliability
Blockchain-based case study of a Smart Home	Ethereum	[50]	PoW	✓	✓	✓	×	Median
SmartEdge- Ethereum	Ethereum	[61]	PoW	✓	×	✓	×	Median
WOT	Ethereum	[62]	PoW	✓	×	✓	×	Median
Blockchain-based Authentication System	Ethereum	[63]	PoW	✓	✓	✓	×	Median
BCoT Sentry	Ethereum	[64]	PoW	×	×	✓	✓	Median
BlockAuth	Hyperledger Fabric 1.4	[65]	PBFT	✓	×	✓	×	Median
DAMFA	Namecoin	[67]	PoW	✓	×	✓	✓	Median
BCTrust	Ethereum	[68]	PoW	✓	✓	✓	×	Median
Blockchain-based User Authentication	Ethereum	[69]	PoW	✓	×	✓	×	Median
Smart District Model	Ethereum	[70]	PoW	×	×	×	×	Concept Paper

but lack strong security and reliability. It needs robust yet reliable solutions that address the issues with these schemes.

As stated in the sections aforementioned, the blockchain-based authentication mechanisms depend on the copy of authentication requests distributed across all the nodes in a decentralized architecture. This property makes it difficult for any possible breach; however, some of the authentication issues have been highlighted that need robust solutions and are discussed under.

The authentication and authorization solution have been proposed based on trusted third-party (TTP) decentralized platforms such as FIWARE, which offers a rich set of open standard APIs to acquire data from the IoT of the smart city but not on the Blockchain itself. In contrast, Blockchain has been utilized merely as a distributed data repository.

  - The reliance on TTP decentralized platform for authentication and authorization mechanism opens doors to adversaries on IoT-enabled smart devices.
  - The communication overheads (in terms of traffic, processing time, and energy consumption) are significantly higher than the base models concerning its security and privacy gains which would need to be considered in time-critical IoT applications.

- Different techniques can extract useful knowledge from big data by filtering, normalizing, and compressing IoT data. The IoT-enabled smart devices involve embedded devices, communication, and target services (Blockchain, cloud); thus, savings in the amount of data that the IoT provides can benefit multiple layers.
  - A local storage device for backup data has been introduced in some of the proposed solutions whose security risks have to be considered in authentication schemes that are open to attack vectors and may jeopardize the network security.
- Smart contracts (SC) define the applications that are decentralized in nature and are special entities that provide real-world data in a trusted manner. The validation process of these smart contracts could be compromised since the IoT-enabled smart devices can be unbalanced.
  - SC in proposed solutions is not designed considering the heterogeneity and constraints present in the IoT-enabled smart devices in the smart city concept.
  - Functions and events in the SCs enable the actuation mechanisms to be employed in the IoT-enabled smart devices much faster.
  - Smart contract deployment with defined authentication functions may provide security, so authentication schemes with smart contacts/decentralized apps (dApps) should be considered.
- The IoT-enabled smart devices have security issues from the manufacturer's perspective as the asset's firmware is not fully equipped with a security mechanism by default.
  - Especially authentication, access control schemes, and firmware updates are commonly found unattended, which poses the exploitation of these assets.
  - Strong and lightweight encryption schemes such as one round cipher etc., would help mitigate the authentication and access control issues based on communication and computational costs.
  - Running applications can be updated using partial upgrades, but the network stack has to be updated by updating the firmware.
    - An effort has been made to update the firmware in run time, such as GITAR [74] and REMOWARE [75] architectures that support these assets in runtime for the network and firmware updates which is essential to ensure a secure integration of the IoT with Blockchain over time.
- Heterogeneity among the assets is yet another issue at the network layer that poses a security threat. Many heterogeneous devices with weak or default security mechanisms operate, send, and receive data. At the same time, the adoption of BC for obvious reasons has proposed BC as a key technology to provide a much-needed security mechanism for IoT-enabled smart devices and the network.

VIII. Recent Advancements & Future Research Directions

This section presents the recent advances and the future challenges conceived from the review papers. In smart city infrastructure, the data is transmitted from multiple CPSs to the security operations center (SOC) over the internet, posing security threats in different communication architectures of the smart city. The security solutions need attention to build robust mechanisms that would eventually safeguard the IoT-enabled smart devices in a smart city concept. Below mentioned recent advances with future research challenges in each section give an overview for future research in industry and academia.

A. Blockchain-As-A-Service (BaaS)

Figure 5 depicts the blockchain-based architecture that adds a BC layer to the generalized smart city layered architecture presented in Figure 4. It integrates IoT-enabled smart devices in blockchain-enabled CPSs (such as smart homes, hospitals, etc.). The blockchain-enabled smart city architecture can be classified into four layers, while the inclusion of the blockchain layer supports robust security mechanisms. As stated in Section 2, the sensing layers deploy the edge and fog nodes (i.e., sensors, aggregators, and actuators) in the

physical environment within cyberspace that supports actuation based on the data collection. Here fog computing provides enough computational resources for data collection and processing for environmental sensing. The network provides connectivity using communication and transmission technologies at the transmission layer. In contrast, the command and control work on the application layer defines the applications for the asset's behavior at the physical layer. As shown in Figure 5, the blockchain layer is of immense importance as it offers Blockchain as a service (BaaS) in a smart city concept.

The underlying DLT and the consensus mechanisms provide robust security for communication that cannot be tempered. The posted data is shared among all the nodes in the BC network, making it decentralized and in an immutable state. This data cannot be altered unless and until the posted data is altered on all the decentralized nodes, requiring a lot of processing and computational overhead. One main concern of the BC layer is to provide security services (CIA & AAA) to the users and CPE (i.e., sensors and actuators) within CPSs in smart cities in a decentralized manner. Apart from centralized architecture, distributed systems have also been in use traditionally. Still, the authentication mechanism for smart cities based on DLT is yet to be explored further for their use in it.

1) Blockchain Tokenization

As shown in Figure 5, the BC layer opens many more opportunities to utilize BC-based services, such as blockchain-based tokenization schemes for asset identification and authentication schemes in smart city architecture. After a huge appreciation of Token creation in 2018, with over 1,132 ICOs and STOs collecting nearly $20bn [76], the concept of Token has gained wide attention. Tokenization in BC presents the concept of digital representation of an asset on the Blockchain or colloquially "programmable money." There are different types of tokens presented by BC tokenization, tangible or intangible, such as security tokens, tokenized securities, utility tokens, and currency tokens (i.e., fungible or non-fungible) [77]. Tokens presented by BC tokenization are algorithms implemented as a Smart Contract on a Blockchain. CryptoKitties is one of the first-ever Ethereum-based collectibles game use cases that deployed tokens in a production environment [78], while other examples of collectibles are available for purchase on NFT marketplaces such as OpenSea [79] and NBA Top Shot [80], etc.

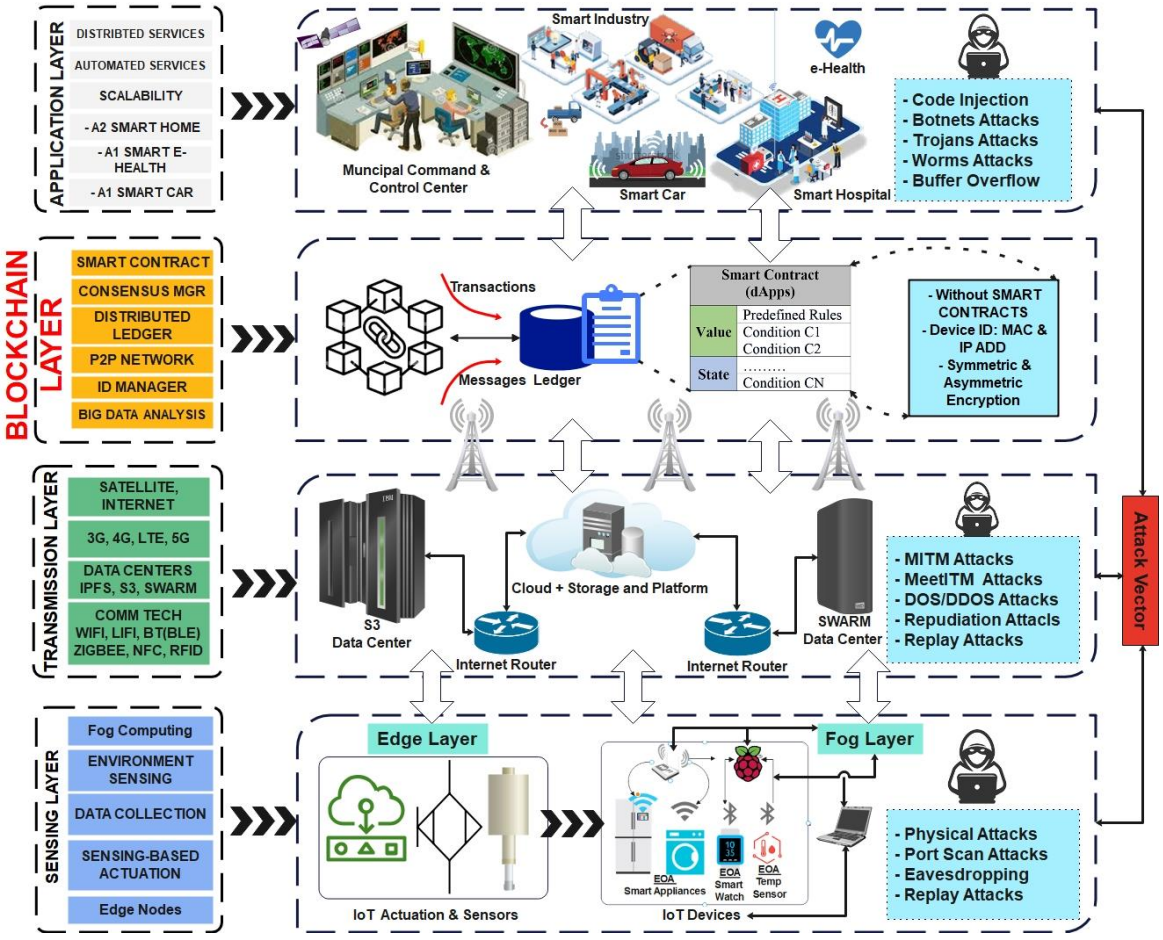

Figure 5. Blockchain-based Smart City Architecture

Since it maintains the data in a secure and immutable state, it has attracted much attention, and a humongous amount of money has been. It is being invested in these virtual collectibles. Individual CryptoKitties are traded at over $100,000 [81]. One of the important aspects of the tokenization for stamps is determining the value by its rarity, and that is how the SC algorithm guarantees uniqueness by mitigating the copies and limiting the maximal number of Tokens available. Ethereum platform has been used to generate Tokens through smart contracts. However, BC tokenization, such as non-fungible tokens (NFTs), leverages decentralized networks through SC implementation, i.e., Ethereum implements the standard based on Ethereum request for comment (ERC-271 and ERC 1155) tokens specification.

B. Non-Fungible Tokens (NFTs)

One popular crypto-tokens utilize the ERC-721 standard defines guidelines on developing non-fungible tokens (NFTs) on the Ethereum blockchain utilizing smart contracts. The NFTs represent the ownership of the physical or digital assets such as physical property, virtual collectibles, or negative value assets. Although the NFTs have been defined under the category of currency tokens, these crypto tokens can be used apart for specified purposes such as Multi Token Standard (ERC-1155) [82]. It allows combining fungible and non-fungible tokens in the same token or standards that support royalty payments (EIP-2981) [83] and mortgage/rental functions (EIP-2615) [84]. We believe these tokens can be used to identify and authenticate assets in a smart city infrastructure where users and devices can be identified by a public key and transact uniquely by the identified tokens.

C. SHA Hashing

SHA (Secure Hash Algorithm) has been used to generate cryptographic hashes for secure communication and record changes in the original data. It exists mainly in four forms of different hash functions such as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 and SHA-1 hash is 160 bits long and has structural similarities to MD5 and MD6 hashing functions. It was developed by NSA (National Security Agency), published in 1995, and released in 2001. It was coded because of many problems in MD5 and MD6 hashing functions and has performed much better comparatively. SHA-2 refers to the hash family of six hash functions such as SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256, while SHA-3 is different [85], [86].

SHA-3, however, is an important breakthrough in the cryptographic arena. It was developed by The National Institute of Standards and Technology (NIST) using a public competition, and nine years in the making, SHA-3 is the new Federal Information Processing Standard (FIPS) 202. A Permutation-Based Hash and Extendable-Output Function employs information security and assures data integrity in digital transactions [87]. This property of SHA-3 has been widely adopted in authentication solutions for deployment. We believe it can be implied for authentication of assets in a smart city infrastructure where users and devices EOAs can be utilized with global variables and public/private keys in a distributed environment, such as blockchain.

D. Research Challenges in BaaS

The concept of Blockchain-as-a-Service (BaaS) has taken a huge appreciation as the use is not limited to cryptocurrency; rather, it has been expanded to multiple domains in the industry and academia. It increases the challenges for its deployment and integration in those domains. Below mentioned are the challenges that have been discussed from a future research challenges standpoint.

1) Security Services: Weaknesses and Threats

Data integrity and availability are the issues with these assets that have to safeguard the huge amount of data that these assets generate. Data integrity and privacy are the key concerns that would help secure the data generated by the IoT-enabled smart devices; however lightweight cryptographic mechanisms are needed keeping in view the resourced-constraint nature of these assets. In case of compromised data integrity, the data uploaded to the BC would stay corrupted. The data uploaded in BC remains immutable and can identify its transformations, e.g., eavesdropping, denial of service or controlling the environment, participants, vandalism, the failure of the devices, etc.

2) Anonymity and Data Privacy

Data anonymity is yet another challenge that can be achieved together with data integrity and privacy by implementing decentralized proxy re-encryption schemes. It would help the message be hidden until decoded by the recipient. Implementing decentralized proxy re-encryption schemes together with BC would strengthen data anonymity. Trust is another key feature of the IoT where blockchain integration can play a role. Efficient and restricted access control for the IoT-enabled smart devices can be achieved by implementing data integrity techniques with an option to ensure data access simultaneously. It is preferable to avoid overloading Blockchain with the huge amount of data generated by the IoT.

3) IoT-enabled Assets Firmware Upgrade

Initiatives for firmware updates in run time would enable the network to have updated assets essential to ensure a secure integration of the IoT with Blockchain.

4) Storage Capacity and Scalability

Blockchain is not a medium for storing large amounts of data like those produced in IoT-enabled smart devices. Only useful data may be extracted out of the humongous data generated by assets for extracting knowledge and making informed decisions, as in the case of actuation actions.

Decentralized storage platforms, such as an interplanetary file system (IPFS), Swarm, and S3, can be utilized. They can be integrated into the BC platform, as in the case of IPFS for Ethereum BC.

5) Integration of IoT-enabled Assets to Blockchain

As discussed in the review, the IoT integration in BC inherits the challenges as these IoT-enabled smart devices are resourced-constraints devices. At the same time, BC's computational overhead for posting transactions causes integration issues. These devices also generate terabytes (TBs) of data in real-time, limiting their integration with Blockchain.

6) Smart Contracts

Overloading is an issue with the SC when accessing multiple data sources, but these contracts' distributed and decentralized nature would provide an edge; however, these SC can be expensive in terms of computation while processing huge computations. The process of filtering and group mechanisms may be incorporated into the SCs. It may enable applications to address the IoT-enabled smart devices depending on the context and requirements of the smart city concept. Interoperability among different cyber-physical systems in a smart city is another factor that needs SC deployments for overall assets and systems.

7) Digital Representation of Assets

Another challenge is the device authentication and digital representation that has been achieved using traditional ways such as the device's MAC or IP addresses. It exposes the devices with their embedded credentials in smart city networks from an adversarial point of view. However, blockchain tokenization can achieve it innovatively, especially with non-fungible tokens (NFTs). It may help mitigate device identification issues by representing and accessing the assets digitally with the help of smart contract functions and events.

E. Cryptosystems

As shown in Figure 6, blockchain-based solutions have been proposed to provide security services (i.e., confidentiality, integrity, availability, and authentication schemes) for data utilizing cryptographic security schemes. It enables the system to attain robust security and privacy for connected parties and their message exchanges. Blockchain-based symmetric (such as DES, AES), and asymmetric cryptographic schemes (such as RSA, ECC, DSS, Diffie-Hellman exchange), have widely been used along with non-cryptographic solutions (such as IDS/IPS, Firewalls and honeypots, etc.) as depicted in Figure 6. However, due to mathematical difficulty in solving the cryptographic hashes and the high communication payload, it has been a challenge to deploy these security schemes in CPSs for smart city infrastructure [69] [61], [88]. These schemes are either dependent on the underlying PKI infrastructure of the Blockchain or PKI-based implementation in a client-server environment or cloud for storing and managing assets.

1) Research Challenges in Cryptosystems

The research to mitigate security challenges in smart cities is mostly focused on authentication; however, in most existing authentication protocols, the trustworthiness for evaluation of IoT-enabled smart devices in smart cities has been ignored. The authentication, authorization, and security services are of immense importance, which can be achieved by implying lightweight and robust cryptographic algorithms for securing communications.

- One-round cipher algorithms have introduced a new generation of cryptographic algorithms with low latency to generate the hashes. It utilizes the dynamic key approach. A dynamic key (that depends on a secret key and a nonce and generates different cipher text for the same plain text) is generated for each input, such as audio, image, or video. The proposed lightweight cipher algorithms are based on a dynamic structure with a single round consisting of simple operations. They can help provide security for time-critical applications for resourced-constraints devices [89], [90].

2) Decentralized Key Management System

The new breed of cryptographic primitives is to be explored based on decentralized architectures such as decentralized key management systems (dKMS) that address the limitations of using consensus networks to store and manipulate private, encrypted data securely.

- Cryptosystems that are **CCA** (security against chosen-ciphertext attacks) secure, while notions of **CPA-security** (security against chosen-plaintext attacks) and **CCA-security** apply to proxy re-encryption.
- An example in this context is NuCypher, which enables sharing of sensitive data for both decentralized and centralized applications, providing security infrastructure for applications from healthcare to identity management to decentralized content marketplaces. It will be an essential part of decentralized applications, just as SSL/TLS is an essential part of every secure web application; thus, security services based on decentralized KMS need to be explored based on blockchain solutions [91].

3) New Breed of One-way Hash Function: SHA-III

Secure Hash Algorithm-3 standard is a next-generation tool for securing the integrity of electronic information. Developed by the National Institute of Standards and Technology (NIST), the SHA-3 specifies a family of functions based on Keccak, which is very different from SHA-2 in design. Though SHA-II has been successfully deployed for hashing without any problems or loopholes, SHA-III adds more strength to the cryptographic family. SHA-3 functions provide a base for deployment to IoT-enabled smart devices as the implementation does not require much of the additional electrical structure on a chip.

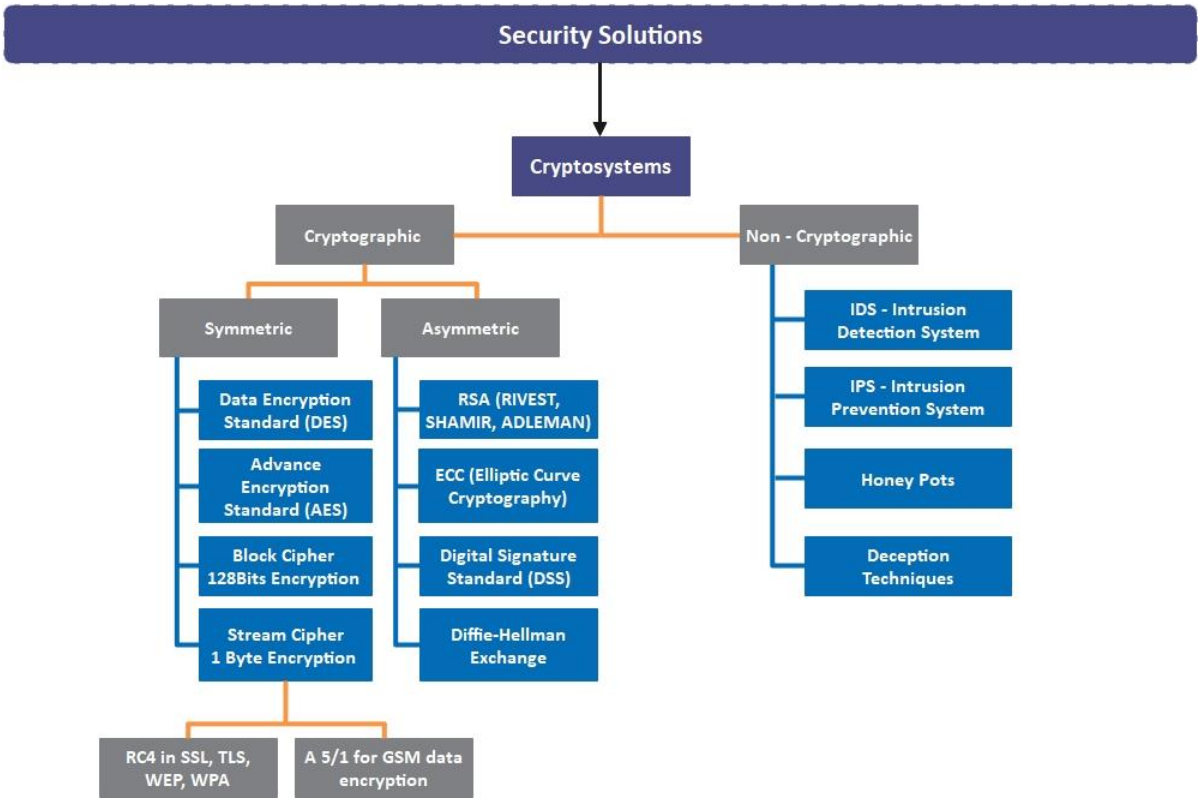

Figure 6. Security Solution-based on Cryptosystems

Hence, it can be useful in providing alternatives for securing very small devices [92].

CONCLUSION

This paper provides an updated literature review of proposed authentication schemes in the IoT context for smart cities. The review poses a large spectrum of authentication schemes that identified many requirements and open issues to be considered by the researchers to develop robust, lightweight schemes. A descriptive approach presents the decentralized architectures for IoT-enabled smart assets that pose threats and need consideration as far as a security standpoint in smart cities is concerned. Considering the resourced-constraint nature of the low-powered IoT-enabled smart assets for the smart city infrastructure, Blockchain (BC)-based solutions and distributed algorithms have to be explored as most of the deployments in a smart city are centralized. It poses threats in terms of a single point of failure and single point of contact from device authentication and overall system's perspective. The BC-based solution has issues in storing data generated by the assets for which the decentralized storage platforms, such as an interplanetary file system (IPFS), Swarm, S3, etc., may be explored. This integration may support storing data hashes to avoid storage exhaustion issues.

A new generation of cryptographic algorithms needs to be developed and deployed to attain robust security services such as data and device anonymity and integrity. The performance evaluation of the new generation of cryptographic algorithms with low latency to generate the hashes should be explored. It will help provide security for time-critical applications keeping in view the resourced-constraints nature of IoT-enabled smart devices. Decentralized key management systems (dKMS) and SHA-III have to be explored in this context to address the limitations of using consensus networks for securely storing and manipulating private, encrypted data can be considered. The identified security issues have been categorized based on authentication architecture and discussed, providing future research challenges accordingly.

ACKNOWLEDGMENT

The author would like to express sincere appreciation for the resources provided by Universiti Brunei Darussalam (UBD), Brunei Darussalam, and the technical assistance and support from the co-authors. Their precious time for the research and their valuable input made it possible to consolidate all this work.

CONFLICT OF INTEREST

The author(s) declared no potential conflicts of interest concerning this article's research, authorship, and/or publication.

REFERENCES

[1] Cisco, "Cisco: 2020 CISO Benchmark Report," 2020. doi: 10.1016/s1361-3723(20)30026-9.

[2] L. Vinet and A. Zhedanov, "A 'missing' family of classical orthogonal polynomials," *J. Phys. A Math. Theor.*, vol. 44, no. 8, pp. 1–11, 2011, doi: 10.1088/1751-8113/44/8/085201.

[3] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors (Switzerland)*, vol. 18, no. 9, pp. 1–37, 2018, doi: 10.3390/s18092796.

[4] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

[5] 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, doi: 10.1109/COMST.2020.2986444.

[6] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015, doi: 10.5120/19787-1571.

[7] BehrTech, "6 Leading Types of IoT Wireless Technologies | BehrTech Blog," *BEHRTECH Technologies Inc*, 2020. https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/ (accessed Apr. 18, 2020).

[8] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[9] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, 2015, doi: 10.1016/j.bushor.2015.03.008.

[10] Sandeep Verma, "Network Topologies in Wireless Sensor Networks: A Review 1," *Int. J. Electron. Commun. Technol.*, vol. 4, no. 3, pp. 1–5, 2013, doi: 10.1.1.308.796.

[11] "PKtronics: Structure of a wireless sensor node :," 2017. http://pktronics.blogspot.com/2017/10/structure-of-wireless-sensor-node.html (accessed Jul. 14, 2020).

[12] E. Wikström and U. M. Emilsson, "Autonomy and Control in Everyday Life in Care of Older People in Nursing Homes," San Jose. CA, 2014. doi: 10.1080/02763893.2013.858092.

[13] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6. pp. 854–864, 2016, doi: 10.1109/JIOT.2016.2584538.

[14] Cisco Academy, "Evolution of Software Defined Networking within Cisco ' s VMDC Challenges within the Data Center SDN Architectural Framework and Solution Characteristics," San Jose. CA, 2014.

[15] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors (Switzerland)*, vol. 19, no. 5, pp. 1–43, 2019, doi: 10.3390/s19051141.

[16] M. M. Rana and R. Bo, "IoT-based cyber-physical communication architecture: Challenges and research directions," *IET Cyber-Physical Syst. Theory Appl.*, vol. 5, no. 1, pp. 25–30, 2020, doi: 10.1049/iet-cps.2019.0028.

[17] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77, p. 103201, 2020, doi: 10.1016/j.micpro.2020.103201.

[18] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustain. Cities Soc.*, vol. 38, no. January, pp. 697–713, 2018, doi: 10.1016/j.scs.2018.01.053.

[19] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, no. 2018, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.

[20] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, 2020, doi: 10.1109/MNET.001.1900178.

[21] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 1, pp. 81–93, 2014, doi: 10.1002/ett.2704.

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[23] M. Keshk, N. Moustafa, E. Sitnikova, B. Turnbull, and D. Vatsalan, "Privacy-preserving techniques for protecting large-scale data of cyber-physical systems," *Proc. - 2020 16th Int. Conf. Mobility, Sens. Networking, MSN 2020*, pp. 711–717, 2020, doi: 10.1109/MSN50589.2020.00121.

[24] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K. K. R. Choo, "A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5110–5118, 2020, doi: 10.1109/TII.2019.2957140.

[25] M. J. Khojasteh, A. Khina, M. Franceschetti, and T. Javidi, "Authentication of cyber-physical systems under learning-based attacks," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 369–374, 2019, doi: 10.1016/j.ifacol.2019.12.183.

[26] H. Wardak, S. Zhioua, and A. Almulhem, "PLC access control: A security analysis," in *2016 World Congress on Industrial Control Systems Security, WCICSS 2016*, 2017, pp. 56–61, doi: 10.1109/WCICSS.2016.7882935.

[27] IETF, "RFC6749-The.OAuth.2," 2012.

[28] K. Weise, "Brian Krebs: The cybersecurity blogger hackers love to hate," *Bus. Week*, Jan. 2014, Accessed: Apr. 15, 2020. [Online]. Available: http://www.businessweek.com/articles/2014-01-16/brian-krebs-the-cybersecurity-blogger-hackers-love-to-hate.

[29] B. Krebs, *Security Fix — Brian Krebs on computer and Internet security*. Voices blogs, The Washington Post, 2009.

[30] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, no. Ml, pp. 29–35, 2018, doi: 10.1109/SPW.2018.00013.

[31] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," in *Proceedings - IEEE Symposium on Security and Privacy*, 2019, vol. 2019-May, pp. 1362–1380, doi: 10.1109/SP.2019.00013.

[32] M. A. Ferrag, L. Maglaras, A. Derhab, and J. B. Bernabe, "Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends," *Secur. Commun. Networks*, vol. 2019, pp. 1–20, 2019, doi: 10.1155/2019/5452870.

[33] D. Sepranos and M. Wolf, "Challenges and Opportunities in VLSI IoT Devices and Systems," *IEEE Des. Test*, vol. 36, no. 4, pp. 24–30, 2019, doi: 10.1109/MDAT.2019.2917178.

[34] R. KumarGoutam, "Importance of Cyber Security," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 14–17, 2015, doi: 10.5120/19550-1250.

[35] M. K. Choi, C. Y. Yeun, and P. H. Seong, "A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology," *IEEE Access*, vol. 8, pp. 118732–118740, 2020, doi: 10.1109/ACCESS.2020.3005134.

[36] M. B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Bus. Insid.*, p. 1, Nov. 2013, Accessed: Oct. 10, 2021. [Online]. Available: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[37] M. D. Cavelty, "Cyber-security," *ResearchGate*, no. May 2012, p. 18, 2014, [Online]. Available: https://www.researchgate.net/publication/256018865.

[38] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry (Basel).*, vol. 11, no. 2, 2019, doi: 10.3390/sym11020293.

[39] OWASP, "Code Injection Software Attack | OWASP Foundation," *owasp.org*, 2021. https://owasp.org/www-

community/attacks/Repudiation_Attack (accessed Jan. 31, 2022).

[40] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," in *arXiv*, 2018, pp. 1–20, [Online]. Available: http://arxiv.org/abs/1801.06275.

[41] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, 2017, doi: 10.1109/JPROC.2017.2686394.

[42] Z. Li *et al.*, "Research on DDoS attack detection based on ELM in IoT environment," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2019-Octob, pp. 144–148, 2019, doi: 10.1109/ICSESS47205.2019.9040855.

[43] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, no. January, p. 102448, 2021, doi: 10.1016/j.adhoc.2021.102448.

[44] H. Noura, S. Martin, K. Al Agha, and K. Chahine, "ERSS-RLNC: Efficient and robust secure scheme for random linear network coding," *Comput. Networks*, vol. 75, no. PartA, pp. 99–112, 2014, doi: 10.1016/j.comnet.2014.09.013.

[45] A. S. Siddiqui *et al.*, "Hardware assisted security architecture for smart grid," *Proc. IECON 2018 - 44th Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 1, no. 1566530, pp. 2890–2895, 2018, doi: 10.1109/IECON.2018.8591401.

[46] P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, 2019, doi: 10.1109/JIOT.2018.2846299.

[47] H. D. Syahla and D. Ogi, "Implementation of Secure Parking Based on Cyber-Physical System using One-time Password Gong et al. Scheme to Overcome Replay Attack," *8th Int. Conf. ICT Smart Soc. Digit. Twin Smart Soc. ICISS 2021 - Proceeding*, pp. 1–6, 2021, doi: 10.1109/ICISS53185.2021.9533246.

[48] K. Sandoval, "OAuth 2.0 – Why It's Vital to IoT Security," 2017. https://nordicapis.com/why-oauth-2-0-is-vital-to-iot-security/ (accessed May 27, 2021).

[49] I. X-Force, "Mirai Botnet Loader Campaign," *IBM X-Force Threat Research*, 2017. https://exchange.xforce.ibmcloud.com/collection/Mirai-Botnet-Loader-Campaign-7e8131a283d50a0f13d43ae5f1d0058b (accessed Apr. 15, 2020).

[50] 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 2017*, 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[51] Z. U. Rehman, S. Altaf, and S. Iqbal, "Survey of Authentication Schemes for Health Monitoring: A Subset of Cyber Physical System," in *Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019*, 2019, pp. 653–660, doi: 10.1109/IBCAST.2019.8667166.

[52] H. Department of the Army, "Supervisory Control and Data Acquisition (SCADA) Systems for command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities," 2006.

[53] J. Finkle and D. Skariachan, "Target cyber breach hits 40 million payment cards at holiday peak," *Reuters US Edition*, vol. Cyber Crim. p. http://www.reuters.com/news/technology/article/201, 2013, Accessed: Oct. 11, 2021. [Online]. Available: https://www.reuters.com/article/us-target-breach-idUSBRE9BH1GX20131219.

[54] "German Steel Plant Suffers Significant Damage from Targeted Attack - Nouvelles de sécurité - Trend Micro FR," *Nouvelles de sécurité - Trend Micro*, 2015. https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack (accessed Oct. 11, 2021).

[55] Z. Wang, X. Dong, Y. Li, L. Fang, and P. Chen, "IoT Security Model and Performance Evaluation: A Blockchain Approach," *Proc. 2018 6th IEEE Int. Conf. Netw. Infrastruct. Digit. Content, IC-NIDC 2018*, pp. 260–264, 2018, doi: 10.1109/ICNIDC.2018.8525716.

[56] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," in *Proceedings of the 13th ACM Symposium on Operating Systems Principles, SOSP 1991*, 1991, pp. 165–182, doi: 10.1145/121132.121160.

[57] Tim Hinrichs, "Centralized vs. Distributed Authorization: The CAP Theorem," *Styra*, 2019. https://blog.styra.com/blog/centralized-vs.-distributed-authorization-the-cap-theorem (accessed Jul. 28, 2021).

[58] L. Yang, X. Y. Liu, and W. Gong, "Secure smart home systems: A blockchain perspective," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 1003–1008, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162648.

[59] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Inf. Process. Manag.*, vol. 58, no. 3, p. 102482, 2021, doi: 10.1016/j.ipm.2020.102482.

[60] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf. Process. Manag.*, vol. 58, no. 2, p. 102468, 2021, doi: 10.1016/j.ipm.2020.102468.

[61] K. L. Wright, M. Martinez, U. Chadha, and B. Krishnamachari, "SmartEdge: A Smart Contract for Edge Computing," in *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, 2018, pp. 1685–1690, doi: 10.1109/Cybermatics_2018.2018.00281.

[62] A. Durand, P. Gremaud, and J. Pasquier, "Blockchain based trust & authentication for decentralized sensor networks," in *IoT '17: Proceedings of the Seventh International Conference on the Internet of Things*, 2017, pp. 1–2, [Online]. Available: http://arxiv.org/abs/1706.01730.

[63] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Comput.*, vol. 23, no. 3, pp. 2067–2087, 2020, doi: 10.1007/s10586-020-03058-6.

[64] L. Gong, D. M. Alghazzawi, and L. Cheng, "Bcot sentry: A blockchain-based identity authentication framework for iot devices," *Inf.*, vol. 12, no. 5, pp. 1–20, 2021, doi: 10.3390/info12050203.

[65] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2116–2123, 2021, doi: 10.1109/JIOT.2020.3037733.

[66] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: Breaking the SAML-based single sign-on for google apps," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1–9, 2008, doi: 10.1145/1456396.1456397.

[67] O. Mir, M. Roland, and R. Mayrhofer, "DAMFA: Decentralized anonymous multi-factor authentication," *BSCI 2020 - Proc. 2nd ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, Co-located with AsiaCCS 2020*, pp. 10–19, 2020, doi: 10.1145/3384943.3409417.

[68] M. T. Hammi, P. Bellot, and A. Serhrouchni, "BCTrust: A decentralized authentication blockchain-based mechanism," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2018, vol. 2018-April, pp. 1–6, doi: 10.1109/WCNC.2018.8376948.

[69] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2019, vol. 2018-Novem, doi:

10.1109/AICCSA.2018.8612856.

[70] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *2017 6th International Conference on Renewable Energy Research and Applications, ICRERA 2017*, 2017, vol. 2017-Janua, pp. 454–461, doi: 10.1109/DISTRA.2017.8191102.

[71] Hyperledger Foundation, "Hyperledger Besu," 2021. https://limechain.tech/blog/hyperledger-besu-explained/ (accessed Jan. 08, 2022).

[72] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–29, 2021, doi: 10.3390/s21020359.

[73] Solana, "Scalable Blockchain Infrastructure: Billions of transactions & counting | Solana: Build crypto apps that scale," 2022. https://solana.com/ (accessed Jun. 05, 2022).

[74] P. Ruckebusch, E. De Poorter, C. Fortuna, and I. Moerman, "GITAR: Generic extension for Internet-of-Things ARchitectures enabling dynamic updates of network and application modules," *Ad Hoc Networks*, vol. 36, pp. 127–151, 2016, doi: 10.1016/j.adhoc.2015.05.017.

[75] A. Taherkordi, F. Loiret, R. Rouvoy, and F. Eliassen, "Optimizing sensor network reprogramming via in situ reconfigurable components," *ACM Trans. Sens. Networks*, vol. 9, no. 2, 2013, doi: 10.1145/2422966.2422971.

[76] G. D. Steve Davis, Daniel Diemers, Henri Arsianian, "4 th ICO / STO Report - A Strategic Perspective," *PWC Rep.*, no. March, 2019, [Online]. Available: https://www.pwc.ch/en/publications/2019/ch-20190308-strategyand-ico-sto-report-q1-2019.pdf.

[77] Cryptopedia, "What Is Tokenization? Blockchain Token Types," 2021. https://www.gemini.com/cryptopedia/what-is-tokenization-definition-crypto-token (accessed Sep. 15, 2021).

[78] J. Castro *et al.*, "CryptoKitties | Collect and breed digital cats!," 2020. https://www.cryptokitties.co/ (accessed May 27, 2022).

[79] Opensea, "OpenSea, the largest NFT marketplace," 2021. https://opensea.io/ (accessed May 27, 2022).

[80] NBA, "NBA Top Shot | Officially Licensed Digital Collectibles," *NBA Top Shot*, 2021. https://nbatopshot.com/ (accessed May 27, 2022).

[81] T. Weingärtner, "Tokenization of physical assets and the impact of IoT and AI," *Eur. Union Blockchain Obs. Forum*, vol. 10, pp. 1–16, 2019, [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/research-paper/convergence_of_blockchain_ai_and_iot_academic_2.pdf.

[82] R. S. W. R. A. C. P. C. J. T. Eric Binet, ""EIP-1155: Multi Token Standard," 2018. Accessed: May 25, 2022. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1155.

[83] J. S. Zach Burks, James Morgan, Blaine Malone, "EIP-2981: NFT Royalty Standard," *Ethereum*, 2020. https://eips.ethereum.org/EIPS/eip-2981 (accessed May 25, 2022).

[84] K. Shiba, "EIP-2615: Non-Fungible Token with mortgage and rental functions," 2020. https://eips.ethereum.org/EIPS/eip-2615 (accessed May 25, 2022).

[85] B. Möller, "Sliding Window Exponentiation," *Encycl. Cryptogr. Secur.*, no. 1982, pp. 1222–1224, 2011, doi: 10.1007/978-1-4419-5906-5_46.

[86] S. Ling, H. Wang, and C. Xing, "Secret Sharing Schemes," *Algebr. Curves Cryptogr.*, pp. 109–154, 2013, doi: 10.1201/b14977-10.

[87] N. R. Chandran and E. M. Manuel, "Performance Analysis of Modified SHA-3," *Procedia Technology*, vol. 24. pp. 904–910, 2016, doi: 10.1016/j.protcy.2016.05.168.

[88] B. Shrestha and H. Lin, "Data-Centric Edge Computing to Defend Power Grids against IoT-Based Attacks," *Computer (Long. Beach. Calif).*, vol. 53, no. 5, pp. 35–43, 2020, doi: 10.1109/MC.2020.2972228.

[89] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia IoT devices," *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18383–18413, 2018, doi: 10.1007/s11042-018-5660-y.

[90] H. Noura, L. Sleem, M. Noura, M. M. Mansour, A. Chehab, and R. Couturier, "A new efficient lightweight and secure image cipher scheme," *Multimed. Tools Appl.*, vol. 77, no. 12, pp. 15457–15484, 2018, doi: 10.1007/s11042-017-5124-9.

[91] M. Egorov, D. Nuñez, and M. Wilkison, "NuCypher: A proxy re-encryption network to empower privacy in decentralized systems," 2018, [Online]. Available: https://koreaoffice-my.sharepoint.com/:b:/g/personal/joonwchoi_korea_edu/ES6MWKcI3IdDostpMkBa098BwFYDUcqlea0QrLa3NdotUQ?e=clWCpn%0Ahttps://koreaoffice-my.sharepoint.com/:b:/g/personal/joonwchoi_korea_edu/ESCciUnA-FJHrJmXMZude7IBO_ArecXRfMMMhLHahMaAzQ?e=YN.

[92] C. Boutin, "NIST Releases SHA-3 Cryptographic Hash Standard | NIST," *NIST*, 2015. https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard (accessed Jun. 05, 2022).

USMAN KHALIL

Mr. Usman Khalil received an MS in Computer Sciences from University Brunei Darussalam (UBD), Brunei Darussalam, in 2019. Currently, he is a Ph.D. scholar in the Mathematical and Computing Sciences School of Digital Sciences at the University Brunei Darussalam. Previously, he worked as a Telecom professional with more than fourteen years of professional experience in various telecom companies in Pakistan and Malaysia. His research interests focus on the exploratory pattern recognition algorithms for the analysis, data mining, clustering, integration of the Internet of Things with cloud computing, and the integration of the Internet of Things with blockchain.

DR. MUEEN UDDIN

Dr. Mueen Uddin is currently working as Assistant Professor in Digital Sciences Program at the Faculty of Science, Universiti Brunei Darussalam (UBD). He completed his Ph.D. in Information Systems from Universiti Teknologi Malaysia UTM in 2013. MS & BS in Computer Science from Isra University Hyderabad Pakistan in 2008 and 2005. Mueen possesses strong research and publication profile and has worked as a research fellow in his previous assignments at Khalifa University UAE and IIUM Malaysia. Dr. Mueen has fifteen (15) years of professional academic experience in several universities in Malaysia, Saudi Arabia, UAE, Pakistan, and Brunei Darussalam and has been teaching various courses in the domain of Cybersecurity and forensics, Information and Network Security, Cloud Computing Infrastructures, and Information Systems. Dr. Mueen has supervised ten (10) masters and more than 45 Undergraduate students for their dissertations and final year projects (FYPs) during his academic career. He has been an evaluator and examiner for many postgraduate, graduate, and undergraduate projects and dissertations in different universities worldwide. Mueen has published more than 90 research papers in high-quality journals and conferences. His research interests include Cybersecurity and Forensics, Blockchain, Information and Network Security, Energy Efficient Cloud Infrastructures, and Information Systems.

Dr. Mueen has completed five (5) research grants in his previous academic and research positions. He has been serving on many editorial boards and is an active reviewer of many international reputable journals and conferences. He has reviewed more than 100 research articles. Some of the journals include IEEE Access, Renewable, and Sustainable Energy Reviews, IEEE Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, IEEE Systems Journal, Computing Journal Springer, International Journal of Global Warming (IJGW), and journal of Supercomputing. Dr. Mueen has also served as a technical committee member and session chair for various international and local conferences in Computer Sciences and Information Systems.

DR. OWAIS AHMED MALIK

Dr. Owais Ahmed Malik is an Assistant Professor in Mathematical and Computing Sciences, Department of Digital Sciences, University Brunei Darussalam (UBD). He completed his Ph.D. in computer science from University Brunei Darussalam (2015), MS in Computer Science from KFUPM, Saudi Arabia (2002), and is a computer system engineer from NED, Pakistan (1998). Dr. Owais has more than ten years of progressive experience in academia and research in computer science and engineering. He has been teaching various undergraduate courses, including machine learning, data mining, machine perception, programming fundamentals, design and analysis of algorithms, software engineering, and operating system in different national/international universities. His research interest includes designing and exploring different intelligent/pattern recognition algorithms to analyze and classify biodiversity and cyber-security data, applied biomechanics, bio-signal processing, and big data analytics. He has published several articles in internationally reputable journals and conferences.

SADDAM HUSSAIN received Bachelor's and Master's degrees from Islamia College, Peshawar, Pakistan and Hazara University, Masehra Pakistan in 2017 and 2021 respectively. He has published 40+ papers in well-reputed journals including IEEE, JISA Elsevier, Cluster Computing, Computer Communication, IoTJ, Hindawi, CMC, and Electronics. He is serving as a reviewer in reputed journals including IEEE Access, International Journal of Wireless Information Networks, Scientific Journal of Electrical Computer and Informatics Engineering, and CMC. His research interests include Cryptography, Network Security, Wireless Sensor Networking (WSN), Information-Centric Networking (ICN), Named Data Networking (NDN), Blockchain, Smart Grid, Internet of Things (IoT), IIoT, Quantum Computing, Cloud Computing, and Edge Computing.