The Proposed Framework and Challenges towards Smart City Implementation

Wan Fariza Wan Abdul Rahman¹,*, Aisha Hassan Abdalla², Md. Rafiqul Islam³

¹Department of Computer Science, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Kelantan Branch, 18500 Machang, Kelantan, Malaysia
²,³Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University of Malaysia, 53100 Gombak, Selangor, Malaysia

*wfariza@uitm.edu.my

Abstract. The recent increment of population in the urban areas requires well-operated and well-managed cities with lots of automation in various aspects of everyday life. The backbone of this smart city is the Internet-of-Things (IoT) technology. This paper outlines the fundamental idea of IoT, followed by its framework for successful smart city implementation. The deployment of a city-scale IoT infrastructure involves heterogeneity of devices (in terms of hardware, software interfaces, communication interfaces and data transmitted), poses new challenges in several aspects including interoperability and security. There are many review articles on smart city proposing various frameworks, each with its own focus area. However, how different domain areas are to be interconnected together, remained questionable. Due to sensible nature of data involved, privacy and security must be ensured, considering secure environment for users’ personal data in transit and storage. These elements must be integrated into the smart city architecture. Additionally, with the increase demand for mobile applications, the issues of mobility and the optimization of resource management are another challenging part in smart city. These issues and several approaches to tackle each of them are also highlighted in brief. Finally, the enhanced framework for smart city considering the security and privacy issues has been proposed.

Keywords: IoT, smart city

1. Introduction

The term smart city can be defined as the urban areas with various types of intelligent devices. The Information and Communications Technology (ICT) solutions are adopted with the purpose of providing enhanced comfort, fast communication, saving of resources and better security for the citizens. In other words, the main objectives are to increase the quality of the services offered to the citizens by making a better use of public resources, while reducing the operational costs. The technical support of Internet-of-Things (IoT) is applicable in the design of smart city such as efficient street lighting, monitoring air quality and discovering emergency routes.

Ten top smart cities in the world are London, New York, Paris, Tokyo, Reykjavik, Copenhagen, Berlin, Amsterdam, Singapore, and Hong Kong [1]. Amsterdam is an example of a well-connected smart city. The smart city initiative has begun in 2009 with over 170 projects. Copenhagen, being known as one of the smartest cities in the world is leveraging open data to develop an innovative intelligent bike...
system. Using embedded sensors, both the riders and administrators are provided with real-time information to monitor and manage air quality and traffic congestion [2].

Understanding the real concept as well as all the requirements is important to ensure a successful development of a working smart city. Many frameworks and architectures have been proposed in the current research for smart city, but the proper integration of security elements with the basic architecture still need to be reviewed.

The main objective of this paper is to propose the enhanced framework for smart city considering security aspects especially privacy of data collection and sharing. However, the development and details implementation phase are out of scope. The rest of this paper is organized as follows. In Section II, the elements of smart city will be presented with related examples for each. In Section III, the related work on framework of smart city will be presented, focusing on each layer involved. Section IV addresses the challenges and issues that may arise with the deployment of a smart city considering heterogeneity, security, mobility and Quality of Service (QoS). Section V highlights the process performed in getting the overall idea of smart city architecture, issues to be tackled and getting all ideas together. This section is then followed by Section VI which presents the proposed of enhanced framework for smart city. Finally, the conclusion is drawn in Section VII.

2. Elements of smart city
The smart city covers seven types of different services, namely (1) Smart Healthcare, (2) Smart Mobility (Smart Transportation), (3) Smart Electricity and Water Distribution (Smart Energy), (4) Smart Environment, (5) Smart People (Citizens), (6) Smart Economy (Smart Industries), (7) Smart Living (Smart Offices and Residential Buildings) [3 – 6], (8) Smart Infrastructure and Smart Agriculture. The following subsections explain each of these services in details.

2.1. Smart Healthcare
Rapid growth of population may cause traditional healthcare to be overwhelmed. Therefore, to cater over increasing demand with limited resources, smart healthcare offers intelligence, efficiency and sustainability to traditional healthcare. The main components of smart healthcare include smart hospitals, smart emergency response and emerging on-body sensors, such as wearable devices and smart biosensors. Access to the patient data can be made in real-time at even different hospitals, allowing the medical staffs, doctors and nurses to make real-time decisions on patient health and corresponding medication.

Two main examples of smart healthcare are telemedicine and assisted living for senior citizens. With the use of ICTs, telemedicine can provide long distance clinical healthcare. This approach is not only beneficial for remote locations where healthcare services are not easily accessible, but also can save lives in emergency situations. Assisted living, on the other hand, allows the senior citizens to enjoy their daily activities with minimal need of skilled nursing care, but still having the medical staffs available for them 24/7.

2.2. Smart Transportation
Smart transportation systems are nowadays possible with the Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P) or Pedestrian to Infrastructure (P2I) technologies. Being known as Intelligent Transport Systems (ITS), smart transportation includes many types of communication and navigation systems in vehicles, between vehicles as well as between vehicles and fixed locations. Smart transportation covers the interactions among railway network, road transport, airline transport and water transport, allowing passengers to choose different transportation options for low-cost, and fastest routes or shortest distance. Not only that, safe, cost-effective, rapid and reliable transportation is possible with the construction of intercity railway networks, intelligent road networks, global airway hubs, and integrated public transport. Trip scheduling in public transport makes use of real-time data for route mapping. Even the driver behavior and traffic patterns can also be tracked using global positioning system (GPS) data.
2.3. Smart Energy
Smart energy refers to the following: smart power generation, smart power grids, smart storage and smart consumption. In other words, smart energy could be defined as the intelligent integration of decentralized sustainable energy sources, efficient distribution and optimized power consumption. Efficient distribution is enabled using smart infrastructure, smart grid, smart meters and ICT. Smart grid is the backbone of a smart energy system by ensuring efficient, economical, and sustainable energy at minimal level of loss, higher quality supply, safety system and users, security of the supply and fault-tolerance of the system. Smart grid uses ICT to support demand-response management of energy consumption such as to effectively synchronize energy from various sources and provide electricity at specific voltage and frequency without fluctuations. Smart metering is an important component of smart grid which records the electric consumption in certain period and communicates that information for monitoring and billing purpose [4].

2.4. Smart Environment
A smart environment covers air quality, green and water spaces, emission monitoring, waste management, energy efficiency and monitoring of city trees. Air quality monitoring and prediction could be achieved through traffic monitoring sensors. Waste management is another significant issue which directly affects the quality of life [5].

2.5. Smart People
The term smart people refers to the connection and communications among citizens to exchange common and imperative online social experiences and share physical space with others. Example can be seen in a crowdsourcing weather application whereby the combination of automatic sensor readings from smartphones and manual input by people are used to assess data on previous, current, and future weather events.

2.6. Smart Industries
Safe working environment for factory workers is one of the main concerns in smart industries. This includes the mechanism for harmful gas detection in factory, as well as the evaluation of machine conditions and workers’ health. Another possible implementation of smart industries is the mobile shopping system targeting the potential shoppers by providing product information that the customer is interested in buying.

2.7. Smart Living (Smart Offices and Residential Buildings)
Smart living defines the improvement in the quality of life of citizens which includes public safety, education, tourism, and healthcare. Considering a crowd-sourcing model and ICT for example, an Interactive Voice Response (IVR) could be used as an effective tool for citizens to report safety problems. Smart buildings on the other hand, involves with the energy consumption management, and interaction with appliances inside the buildings (homes or offices) to provide safety and comfort to the users. Smart building easily adapts its energy demand according to user activities, providing low-cost power utilization. As an example, the air-conditioner or light is automatically switched off when nobody detected in certain area.

2.8. Smart Infrastructure
Smart infrastructure refers to the utilization of sensors for monitoring buildings, roads, and bridges structural state for the purpose of predictive maintenance of the essential units. This is to ensure that their infrastructure is in shape with uninterrupted usage.

2.9. Smart Agriculture
Smart agriculture is crucial to ensure that food production is made sustainable to satisfy the increased number of world population. Smart agriculture involves sensors being placed in plants and fields for
monitoring purpose with targeted measurements. Thus, the targeted care mechanisms can be deployed to prevent diseases as well as that dwindling resources such as water can be utilized efficiently.

3. Related work on framework for smart city

Smart city revolves around extremely diverse range of devices, technologies, and services with high degree of interdependence between various components. Thus, to understand the functionality of smart city, its general architecture needs to be understood first.

Three basic layers of the smart city architectures as highlighted in [6] are sensor layer, network layer and service layer. The sensor layer consists of the various sensors deployed for measuring and monitoring environmental factors such as sound, temperature, and brightness. The network layer provides the communication infrastructure to deliver the data from the sensor layer to the respective actuators. The actuator layer provides reaction for a physical change in the environment via the required service.

In [7], the smart city applications are mentioned to be made up of four aspects: collection of data, exchange of data, storage and analysis. The collection of data is related with the sensor layer mentioned previously, requiring sensor development in the various domains. The exchange of data involves with data transmission from the data collection units (i.e., sensors) towards the cloud for storage and analysis. Data either on a local level or a global level are conveyed by various types of local networks in combination with city-wide Wi-Fi networks, 4G and 5G technologies. At the next stage, different storage schemes are used in the cloud to arrange and organize data, make it usable for the data analysis process. The collected data are then fed into the data analysis stage. The extraction of patterns and inferences ranging from simple analysis for basic decision making, up to more complex ones, using the statistical methods, and real-time machine and deep-learning algorithms.

Another framework for smart city proposed in [23] as shown in figure 1 includes IoT network infrastructure, middleware layer and application layer.

![Figure 1. General framework for smart city services proposed in [8].](image-url)

The IoT network infrastructure includes various types of networks consists of heterogeneous peripheral nodes such as sensors, actuators, and Radio Frequency Identification (RFID) tags for the purpose of data monitoring/collection from the surrounding environment in smart city services and response of events/alerts to the environments (through notifications). The main components of network infrastructure include Wide Area Network (WAN), IoT network, IoT nodes, sensor cloud, gateway, wireless sensor network (WSN) gateway, Wi-Fi access points (APs) and control server. The WAN acts as the backbone of network infrastructure which provides Internet connection throughout the city, whereby the IoT network refers to various IoT nodes for monitoring and collecting the data. All smart devices, sensor nodes, actuators and RFID tags are referred to as IoT nodes.
Sensor cloud can be defined as a scalable and powerful massive storage infrastructure in combination with sensor networks for real-time processing, storing and analyzing the WSN data. The end devices are interconnected to the main communication infrastructure by the gateway which is responsible for protocol translation. The functional mapping is performed by the gateway between the constrained protocols (such as Hypertext Transfer Protocol (HTTP) and IPv4/IPv6) and constrained application protocol (such as Constrained Application Protocol (CoAP) and IPv6 over Low Power Wireless Personal Area Network (6LoWPAN)) associated with IoT peripheral nodes. The control server is deployed to store the huge collection of data in internal database which then will be processed and analyzed.

Dealing with heterogeneous technologies, the middleware layer is required to manage the underlying heterogeneous types of IoT networks. Suitable interfaces for the creation, management and discovery of various services as well as subscription to services is provided by collecting data in different formats via some network management Application Programming Interface (API) and data API. The preprocessing and filtering of data is performed at the middleware layer before data is passed to the application layer. Additionally, some security feature is also enabled to ensure secure environment for different smart services. The application layer consists of smart client applications to invoke various smart city services. It also requires for scalable database systems to store necessary data.

The detailed flow on how data from sensors is processed is shown in figure 2. At level 1, the raw information collected by the sensors is stored for further processing. Since the raw information comes in various formats, they will be converted into a common format, e.g., Resource Description Framework (RDF).

![Figure 2. Multi-level smart city architecture [9].](image)

The conversion format at level 2 begins with summary of the information gathered at level 1 based on transmission, analysis and fusion using semantic web technologies. RDF is commonly used for exchanging information over the web since it facilitates heterogeneous data sharing and integration among different domains. The RDF data then will be utilized by different software applications for intelligent reasoning operations. The data integration and reasoning are performed at level 3. An RDF query language known as SPARQL is used for the purpose of querying, retrieving, and manipulating data/records stored. After the data has been classified, Data property and Object property can be used to form relationships between classes. Sensor data from different domains are combined, which later enables activity recognition and learning new knowledge. At level 4, the inferred data from level 3 is utilized by different web applications for intelligent operating conditions to produce input, output, messaging, alerts, and warnings.
Other than the previously mentioned, various framework and architecture are proposed for smart city with different names of layer, but with similar functionalities and concerns. Table 1 summarizes the proposed architecture for smart city from the current research.

**Table 1. Summary of the proposed architecture for smart city from the literature.**

| Concerns/Approaches                               | Layers                                                                 |
|--------------------------------------------------|------------------------------------------------------------------------|
| A. Arun (2020) IoT functional layers              | Sensing layer, connectivity layer, aggregation layer, platform layer,  |
|                                                  | application layer, enterprise integration layer, visualization layer   |
| Syed et. al (2021) [7], Gheisari (2019) [11],    | Privacy-preservation                                                  |
| Mohamed et. al (2019) [12] & Dutta et. al (2017)| Edge computing, fog computing and cloud computing                    |
| Badii et. al (2019) [14]                         | Mobility, privacy and security                                        |
| Malche et. al (2019) [15]                        | Data integrity and authenticity                                       |
| Sharma & Park (2018) [16]                        | Security and privacy; blockchain-based hybrid network architecture     |
| Park et. al (2018) [17]                          | Quick response                                                        |
| Xia et. al (2020) [18]                           | Heterogeneity and flexibility                                         |
| Qureshi et. al (2020) [19]                       | Security; intrusion detection and prevention system                    |
| Qasem et. al (2020) [20]                         | Heterogeneity, real-time delay                                        |
| Zhang et. al (2020) [21]                         | Big data processing, scalability                                      |
| Hernández et. al (2020) [22]                     | Interoperability, openness                                            |
| Kalajdjeski et. al (2020) [23]                   | General layer model                                                   |
|                                                  | Sensor, gateways, cloud, third party, security layer                  |
4. Challenges

Designing the smart city requires the provision of Internet connectivity among devices with various features, characteristics, and capabilities, applying heterogeneous technologies for collecting and processing data. Even the usage of data in the distributed environments poses new privacy and security consideration. The challenges arise are detailed below:

4.1. Heterogeneity

IoT enables seamless communication flows between heterogeneous devices with different capabilities such as energy availability, processing power and bandwidth requirement. The IoT devices can be classified into high-capacity and low-capacity devices. High-capacity devices with large storage and high processing power (such as air conditioner, smartphone, and tablet) are commonly placed in environments and have direct interaction with human users. Low-capacity devices with small storage and low processing power (such as sensor, temperature controller and meter) usually do not require direct interaction with the users.

In smart city, there are multiple wireless technologies (such as Wi-Fi, Long Term Evolution (LTE)), multiple protocols (such as 6LoWPAN, ZigBee, WirelessHART, Bluetooth Low Energy) and multiple addressing schemes (such as IPv6 128-bit addressing, Bluetooth 48-bit addressing, RFID addressing and EUI-64) in use [24 – 25]. Both IP and non-IP interfaces should be supported to ensure interoperability and smooth communication among devices with multiple interfaces [26]. The most common wireless networking protocols used in smart city are RFID, Near Field Communication (NFC), Bluetooth, Z-Wave, Li-Fi, Wi-Fi, Zigbee, Wi-SUN, Cellular, LoRaWAN, 6LoWPAN, SigFox, and NarrowBand-IoT (NB-IoT). The comparison of these network technologies in term of frequency, data rate, range and topology can be seen in [7].

Automatic assignment of IPv6 addresses to devices which do not support IPv6 or IPv4 could be considered as a solution. A mapping mechanism proposed in [27] to enable stateless address autoconfiguration for legacy technologies by creating modified Extended Unique Identifier-64 (EUI-64) format Interface Identifiers for links or nodes with IEEE EUI-64 Identifiers as well as IEEE 802 48-bit MACs.

Heterogeneity of data can also be seen in raw information collected from sensors. Some of the formats are csv, tweets, text messages and database schemas. The collected formats will be converted into a common format after being processed using semantic web technologies [9].

4.2. Addressing Method

In smart city IoT network, each device needs to be identified and different address must be allocated. The IP connectivity between the global IPv6 networks and 6LoWPANs is necessary. The interoperability between 6LoWPANs devices and external IPv6 network is proposed in [28] through the mapping of 16-bits short address. The Adaptation Identifier (AID) assignment mechanism is applied at the gateway to support multiple network prefixes and to map unique IPv6 address to AID with short length. The IoT devices can also be assigned with the DNS name for easy identification, monitoring and remote controlling. The autoconfiguration of DNS name is based on the device’s category and model [29].

4.3. Security

The smart city is based on the architecture of IoT platforms which involve with huge amount of data exchanged among parties, and the heterogeneity of the protocols and devices. Due to the new type of remote interaction and automation, new security and privacy issue will rise.

4.3.1. Data Privacy

The captured data from smart city, transmitted over IoT networks must be secured from cyber-attacks that might disable the whole city functions, create catastrophic harm or steal personal data. Due massive sensitive information about users gathered by the huge number of IoT devices, the data readings about
a person are treated as personal assets. Any leakage may reveal owner's geological location, health status, and living habits to attackers who may extract desired information and disclose personal privacy. The continuously collected data about the activity of people may expose them to unwanted parties and the data might be used for targeted advertising without their approval. RFID systems for example never authenticates the reader and by default, the tags are set to respond to the interrogation of any compliant reader. The usage of RFID tags might cause privacy concerns since the tags could be accessed and tracked by anyone. To prevent unauthorized user tracking, privacy aware identifiers must be considered. Information such as types of devices, location, usage, amount and type of exchanged data as well as mobility patterns should be protected by only disclosing required information to the authorized party [30 – 31]. Several measures could be considered to protect data privacy. Personal data should be stored in an encrypted way to prevent (in case of breach) the identification of specific compromised data. The users should be given the ability to manage their own personal data and require the erasure of them from the platform if they are willing to. At higher level, automated approach to detect tampered or leaked data in short time should be implemented. The authenticated connections and secure communications need to be established among devices, applications and storage [32].

4.3.2. Security model
The operation of smart city network over heterogeneous technologies, applications and multiple devices with different capabilities requires the basic security building blocks to provide authenticity, interoperability and secure communications. However, the security approach for traditional network is not all appropriate for IoT networks due to node resource constraints. For this reason, the secure IoT architecture for smart city can be categorized into four basic building blocks; (1) Black Networks for data privacy, integrity, confidentiality and authentication; (2) Trusted Third Party (TTP) for efficient and anonymous routing; (3) Unified Registry for maintaining a database of devices; and (4) Key Management for an external key management system [24].

A blockchain-based innovative framework for privacy-preserving and secure data sharing in a smart city environment known as PrivySharing is proposed in [33]. The blockchain network is divided into various channels to implement data privacy preservation. Each channel consists of a finite number of authorized organizations and processes a specific type of data such as smart building, health, smart energy, smart transportation or financial details. The access control rules are embedded in the smart contracts to control access to users’ data within a channel. In addition, further isolation is imposed on the data within a channel by using private data collection and encrypted. Dual security in the form of an API Key and OAuth 2.0 is implemented in the Representational State Transfer (REST) API to enable the interaction between clients and the blockchain network.

Another blockchain proposed method can be seen in [34] where prediction of driver intent and prevention of traffic congestion are possible using digital twin-centric approach. The digital twin terminology refers to the cloud-based dynamic virtual representation for each of the physical systems.

The proposed architecture of edge computing and blockchain enabled participatory smart city applications is highlighted in [35]. Blockchain technology has a great potential since it can be developed to provide verification and traceability of data, authentication and authorization, as well as privacy assurance of personal data. The addition of a new block is event driven, performed by only the authorized citizen. The corresponding node evaluates and verifies all individual transactions before appending any transaction to the chain.

4.4. Mobility Issues
Mobility has become an important requirement in numerous IoT applications. In health monitoring for example, the sensors are equipped at the patients’ body, who can freely move inside a hospital, to transmit data continuously. The topology of the network is dynamic and continuously changing due to the movement of the nodes. The proposed standard protocol for IoT, namely IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is efficient for static environment, but supports reduced mobility [36]. A huge challenge is to provide fast seamless mobility detection while some of the nodes might
even change their location while being in sleep mode. Further, due to resource constraint (highly reduced power and memory) of IoT devices, the mobility support should be implemented without high signalling cost at end devices [37]. Various approaches could be considered to enhance the mobility support including sensor nodes’ movement prediction based on speed classification [38] and Bayesian inference [39] as well as the application of different mobility models for different mobility scenarios [40].

4.5. QoS requirements

IoT network presents different QoS requirements from conventional homogeneous networks due to dynamic and heterogeneous networking environment. The heterogeneity of network consists of multi-service and various applications which refers to the existence of multiple traffic types. The IoT devices generate the traffic patterns with different characteristics, ranging from an intermittent and bursty traffic generated by smart meters, to a continuous traffic resulting from video streaming. Thus, it is crucial for a single IoT network to be able to support all the applications without compromising QoS for any of them. For this purpose, the network traffic can be categorized into two main types with different QoS requirements; (1) throughput and delay tolerant elastic traffic, and (2) the bandwidth and delay sensitive inelastic (real-time) traffic [41]. Different IoT applications have different QoS. Common applications such as home automation and building control [42 – 43], smart meter and environmental monitoring [44], as well as industrial applications [45] all have their own QoS requirements.

4.6. Optimization of resource management

When it comes to constrained IoT devices, resource management plays a vital role. The routing protocol has big implications on network resources such as memory capacity and battery power of the nodes, as well as the available bandwidth. The Node Ability of Participation (NAP) protocol [46] should be considered so that the sensor devices can be adaptive and efficient for different unpredicted situations. The devices dynamically decide their ability in term of energy consumption, link range, battery capacity and so on to continue participation in the network’s activities. Further, dynamic resource scheduling [47] with respect to resource load history data and current load status can also be implemented to reduce the unbalanced load among the devices.

5. Methodology

A detailed methodology to propose the enhanced framework for smart city is shown in figure 3. The literature review is performed on the current related work of basic framework and architecture of smart city. The challenges and issues faced in the implementation of smart city are identified. Since security and privacy issues are two important elements to tackle, possible solutions are identified. The suitable approach is considered to address these issues. The integration of the identified approach and the existing architecture is formulated. Finally, the enhanced framework for smart city considering security aspect is then proposed.
Figure 3. Methodology used.

6. Results and Discussions

The enhanced framework proposed as shown in figure 4 is the result of the integration of the existing basic architecture in [10] with a blockchain-based framework proposed in [35] and [16] for privacy-preserving and secure IoT data sharing. Three basic layers involve are device deployment layer, network layer and application layer.

The device deployment layer consists of the common devices required in the smart city including personal devices, sensor node, actuator, gateway, access point and router. This layer exchanges raw data and real-time response with the upper layer, which is the network layer.

The network layer is responsible to perform the blockchain-based security through encryption, device authentication and authorization. The whole network is based on the distributed architecture divided into two types: core network and edge network. The edge network represents district network, while the core network represents the main city network. The administrators of both city and district maintain their own ledger which is based on the blockchain approach as presented in [16]. The idea is the edge node with limited storage and computation power pre-processes the raw data which is uploaded by the end devices. The data is filtered to gain useful information. The pre-processed encrypted data (when necessary) will be forwarded to the core network. Any transaction request from the device/user also will be sent by the edge node to the miner in the core network. The miner is responsible to ensure the integrity of the information using digital signature and stored hashes. A new block is created by iteratively hashing the information consisting of the previous ID, created block ID, date and time stamp, verified transaction, and digital signature of the miner. An updated blockchain is then sent to all edge nodes and the requested services is provided to the IoT devices/users.

As proposed by [35], Certificate Management Service (CMS) is deployed by the City Administrator to issue X509Certificate to all the resources including citizens, users, services and components. Each distributed ledger has its own local security credentials (in the form of private key and public key) and its X509Certificate, certified by the CMS. The blockchain-based mechanism is also applied to publish and make these certificates available across the domains.

Finally, on top of all the layers is the application layer which handles the interaction between the users/citizens and various smart services. This layer is responsible to manage the device, configure and
manage the content, store and manage the data and perform data streaming and processing. Additionally, the log management and security in term of authorization and authentication are also taken care by this layer.

![Diagram of the proposed general architecture for smart city with blockchain-based security approach](image)

**Figure 4.** The proposed general architecture for smart city with blockchain-based security approach

7. **Conclusion**

The sensor-based technologies in IoT are the key to connect the world, making human life smarter and comfortable. Thus, having proper understanding and planning is crucial to achieve this purpose. The implementation of successful smart city requires for serious consideration to be given to various aspects including interoperability, security and privacy issues. The purpose is not only to provide efficient use of resources, but to guarantee secure, sustainable, and comfortable environment for the citizens. Therefore, the main contribution of this paper is the highlighted challenges faced in the implementation of smart city as well as the proposed enhanced framework considering security and privacy issues. It is hoped that this paper could serve as a guide to the better developments of smart city framework and architecture.

As future work, before final implementation and deployment, the simulation-based experiment could be considered to test the practicality of the proposed framework and architecture in terms of interoperability and tackling security and privacy issues in smart city. This is to ensure that the feedback obtained can be used for further improvement of the overall architecture.

**References**

[1] Forbes 2020 These are the 10 smartest cities in the world for 2020 8 July 2020 https://www.forbes.com/sites/iese/2020/07/08/these-are-the-10-smartest-cities-in-the-world-for-2020/?sh=58bdac7312a

[2] Thales Group 2021 Building a future we can all trust, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart cities

[3] Singh Y, Bhattacharya S and Singh B 2016 IoT: Framework for smart city *Int. J. Pharmacy Technology* 8 4 pp 25432–9

[4] Mohanty S P, Choppali U and Kouganios E 2016 Everything you wanted to know about smart
cities IEEE Consumer Electronic Magazine 5 3 pp 60–70

[5] Kirimat A, Krejcar O, Kertesz A and Tasgetiren M F 2020 Future trends and current state of smart city concepts: A survey IEEE Access 8 pp 86448–67

[6] Laufs J, Borroni H and Bradford B Security and the smart city: A systematic review 2020 Sustainable Cities and Society 55 pp 1–51

[7] Syed A S, D. Sierra-sosa, Kumar A and Elmaghraby A 2021 IoT in smart cities: A survey of technologies, practices and challenges pp 429–475

[8] Sadhukhan P 2019 An IoT based framework for smart city services Proc. 2018 Int. Conf. Communication Computer Internet Things, IC3IoT 2018 pp 376–9

[9] Gaur A, Scotney B, Parr G and McClean S 2015 Smart city architecture and its applications based on IoT Procedia Computer Science 52 1 pp 1089–94

[10] Arun A 2021 Architecting IoT for smart cities Smart Cities in Application pp 141 – 152

[11] Gheisari M, Pham Q, Alazab M, Zhang X and Srivastava G 2019 ECA: An edge computing architecture for privacy-preserving in IoT-based smart city IEEE Access 7 15779 – 86

[12] Mohamed N, Al-Jaroodi J and Jawhar I 2019 Towards fault tolerant fog computing for IoT-based smart city applications 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. pp 752–757

[13] Dutta J and Roy S 2017 IoT-fog-cloud based architecture for smart city: Prototype of a smart building 7th Conference on Cloud Computing, Data Science & Engineering pp 237–242

[14] Badii C, Bellini P, Difino A and Nesi P Privacy and security aspects on a smart city IoT platform 2019 2019 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Commun. Cloud Big Data Comput. Internet People Smart City Innov. pp 1371–1376

[15] Malche T, Maheshwary P and Kumar R 2019 Environmental monitoring system for smart city based on secure Internet of Things (IoT) architecture Wirel. Pers. Commun. 107 pp 2143–72

[16] Sharma P K and Park J H 2018 Blockchain based hybrid network architecture for the smart city Futur. Gener. Comput. Syst. 86 650 – 5

[17] Park S et al 2018 Design and implementation of a smart IoT based building and town disaster management system in smart city infrastructure Appl. Sci. 8 2239 – 49

[18] Xia X, Liu C, Wang H and Han Z 2020 A design of cyber-physical system architecture for smart city Advances in Intelligent Systems and Computing 1031 pp 967 – 973

[19] Naseer K, Awais Q, Francesco A, Giampaolo P and Gwanggil C 2020 Nature-inspired algorithm-based secure data dissemination framework for smart city networks conventional rural areas for seeking economical Neural Comput. Appl. 33 10637 – 56

[20] Ahmad M, Qaseem H, Natouryeh H and Alzaghoul E 2020 Fog computing framework for smart city design International Journal of Interactive Mobile Technologies (iJIM) 14 1 pp 109 – 125

[21] Zhang C 2020 Design and application of fog computing and Internet of Things service platform for smart city Futur. Gener. Comput. Syst. 112 pp 630–640

[22] Hernández J L, García R, Schonowski J, Atlan D, Chanson G and Ruohomäki T 2020 Interoperable open framework for the implementation of standardized urban platforms Sens. 20 2402 pp 1–23

[23] Kalajdjeski J, Korunoski M, Risteska Stojkoska B and Trivodaliev K 2020 Smart city air pollution monitoring and prediction: A case study of Skopje ICT Innovations 2020 (CCIS vol 1316) ed V. Dimitrova and I. Dimitrovska (Switzerland AG: Springer Nature) pp 15–27

[24] Chakrabarty S and Engels D W 2016 A secure IoT architecture for smart cities 2016 13th IEEE Annual Consumer Communication Network Conf. CCNC 2016 pp 812–3

[25] Hoon Kim T, Ramos C and Mohammed S 2017 Smart city and IoT Future Generation Computer System 76 pp 159–62

[26] Lee G M, Park J, Kong N, Crespi N and Chong I 2013 The Internet of Things-Concept and problem statement draft-lee-iot-problem-statement-05.txt pp 1–19

[27] Rizzo G, Jara AJ, Olivieri A, Bocchi Y, Palattella MR, Ladid L, Ziegler S and Crettaz C 2015 IPv6 mapping to non-IP protocols draft-rizzo-6lo-6legacy-02 pp 1–13

[28] Kahng H K, Choi D and Kim S 2011 Global connectivity in 6LoWPAN draft-kahng-6lowpan...
global-connectivity-01.txt pp 1–11

[29] Jeong J and Park J 2016 DNS name autoconfiguration for Internet of Things devices draft-jeong-homenet-device-name-autoconf-03 pp 1–12

[30] Garcia-Morchon O, Kumar S, Keoh S, Hummen R and Struik R 2014 Security considerations in the IP-based Internet of Things draft-garcia-core-security-06 pp 1–45

[31] Medaglia C M and Serbanati A 2010 An overview of privacy and security issues in the Internet of Things Internet of Things 20th Tyrrhenian Workshop Digital Communication pp 389–95

[32] Badii C, Bellini P, Difino A and Nesi P 2020 Smart city IoT platform respecting GDPR privacy and security aspects IEEE Access 8 pp 23601–23

[33] Makhdoom I, Zhou I, Abolhasan M, Lipman J and Ni W PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities 2020 Comput. Secur. 88 p 101653

[34] Kumar S A P, Madhumathi R, Chelliah P R, Tao L and Wang S 2018 A novel digital twin-centric approach for driver intention prediction and traffic congestion avoidance J. Reliab. Intell. Environ. 4 199 – 209

[35] Khan Z, Abbasi A G and Pervez Z 2020 Blockchain and edge computing–based architecture for participatory smart city applications Concurr. Comput. 32 12 pp 1–20

[36] Hoghooghi S and Javidan R 2020 Proposing a new method for improving RPL to support mobility in the Internet of things IET Networks 9 2 pp 48–55

[37] Shin M, Camilo T, Silva J and Kaspar D 2008 Mobility Support in 6LoWPAN draft-shin-6lowpan-mobility-01 pp 1–21

[38] Somaa F, El Korbi I and Saidane L A 2016 Mobility support over RPL using sensor nodes speed classification Proc. IEEE/ACS Int. Conf. Computing System Application AICCSA

[39] Somaa F, El Korbi I, Adjih C and Saidane L A 2016 A modified RPL for wireless sensor networks with Bayesian inference mobility prediction 2016 Int. Wireless Communication Mobile Computing Conf. IWCMC pp 690–5

[40] Kabilan K, Bhalaji N, Selvaraj C, Kumaar B M and Karthikeyan P T R 2018 Performance analysis of IoT protocol under different mobility models Computer Electrical Engineering 72 pp 154–68

[41] Jin J, Gubbi J, Luo T and Palaniswami M 2012 Network architecture and QoS issues in the Internet of Things for a smart city pp 974–9

[42] Martocci J, De Mil P, Riou N and Vermeylen W 2010 RFC 5867 - Building automation routing requirements in Low-Power and Lossy Networks pp 1–26

[43] Brandt A, Baccelli E, Cragie R and Van der Stok P 2015 Applicability statement: The use of the RPL protocol suite in home automation and building control draft-ietf-roll-applicability-home-building-10 pp 1–32

[44] Dohler M, Watteyne T, Winter T and Barthel D 2009 RFC 5548-Routing requirements for urban low-power and lossy networks pp 1–21

[45] Pister K, Thubert P, Dwars S and Phinney T 2009 RFC 5673-Industrial routing requirements in low-power and lossy networks pp 1–27

[46] Baryun A 2015 The node ability of participation (NAP) draft-baryun-roll-nap-00.txt pp 1–8

[47] Chen R 2019 Effective scheduling simulation of Internet of Things load balanced sharing of resources 2019 IEEE 5th Int. Conf. Computer Communication ICC 2019 pp 2136–40