ASTES

*Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 2, 99-112 (2021)*

*www.astesj.com*

*Special Issue on Multidisciplinary Sciences and Engineering*

**ASTESJ**

**ISSN: 2415-6698**

# Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review

Zarina Din*, Dian Indrayani Jambari, Maryati Mohd Yusof, Jamaiah Yahaya

*Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, 43600, Malaysia*

ARTICLE INFO

*Article history:*
*Received: 25 December, 2020*
*Accepted: 20 February, 2021*
*Online: 10 March, 2021*

*Keywords:*
*Smart Cities challenges*
*Internet of Things utilization*
*Information systems management*
*Cybersecurity*

ABSTRACT

*Sustainable urban development and utilization of Internet of Things (IoT) technology is driving cities globally to evolve into Smart Cities (SC). The power of IoT services and applications will enable public agencies to provide personalized services to the citizens and inevitably improves their much-needed quality of life. However, although the use of IoT technology proves to be advantageous to citizens, it is not without challenges, particularly concerning with the management of information security. As agencies prepare towards SCs with the utilization of IoT, their Information Systems (IS) security management is even more critical. Current IS security management approaches must be reviewed and potentially revise appropriately in tandem with the increasing commercial use of the IoT technology. Therefore, this paper aims to discuss challenges in the IS management specifically in protecting and assuring information accuracy and completeness. Document analysis on relevant literature has been carried out to identify and analyse the challenges. The result discusses that the IS security management for IoT-enabled SC is challenged in five aspects: governance, integrity, interoperability, personalization, and self-organizing. Considerations of these challenges will support SC development concerning the IS security management in IoT-enabled SC.*

## 1. Introduction

This paper is a revised and expanded version of a paper entitled Challenges in Managing Information Systems Security for Internet of Things-enabled Smart Cities [1] presented at the 6th International Conference on Research and Innovation in Information Systems (ICRIIS2019). This is a much-refined work of previous studies on Information System (IS) and Internet of Things (IoT) security issues of Smart City (SC) ecosystems.

The total of population living in cities has increased from 746 million in 1950 to nearly 3.9 billion in 2014 [2]. This figure is estimated to increase to more than 6 billion by 2050 [3]. Therefore, several cities are rapidly growing into mega cities. For example, more than 10 million people expand from 10 mega cities in 1990 to 41 mega cities in 2030. Consequently, there will be several problems with the governance of these mega cities, and providing their citizens with a reasonable quality of life. The transformation into Smart Cities (SC) is a realistic approach that some cities are either working on or considering in [2, 4].

SC are very much reliant on information collection and analysis. To provide smart features that help strengthen performance and quality of life, smart systems using IoT technology are introduced and installed. This creates an immense data repository representing several aspects of SC operational activities. The SC services are based on a centralized architecture, where a complex and heterogeneous set of devices embedded over the urban area generates different-centralized architecture data types that are then delivered to a control center through appropriate communication technologies, where data storage and processing are implemented [5]. An SC is a complex system, which means that any security concern could impact the protection of its citizens valuable information [4].

Therefore, IS security management will become a high priority in SC operation to ensure that the transaction of information is secure, accurate, and reliable. In order to avoid unauthorized entries, modifications, thefts, or physical harm to the IS, policies, procedures, and technological measures have been applied [6]. They are vulnerable to many forms of attacks, with a

*Corresponding Author: Zarina Din, p90639@siswa.ukm.edu.my

vast amount of data stored in electronic form and via communication networks as multiple IS are integrated.

IoT technology offers many exceptional prospects for developing applications beneficial to the development of SC, such as intelligent transport and smart public safety. These applications are able to support better quality of life for citizens, efficient use of the SC assets, and also supports sustainability. While integrated IS in SC through these potential IoT applications may offer benefits, , security threats constitute a major barrier. They are exposed to potential security threats toward its urban infrastructure, service quality to its citizens, efficiency in resource utilization, and decrease IS stability. There are several difficulties in detecting, assessing, and avoiding a security threat. Furthermore, the issues involved with threats on integrated IS can cause harm and reduce associated risks of the attacks [7].

With IoT technology growth and market pressure, demands for smart devices have increased, and may result in growing communication among these smart devices in SC. It is anticipated that 125 billion devices will be linked by 2030 [8]. However, without considering security aspects for the deployment of these devices [9], such communication introduces new security risks. In addition, the existing IoT architecture does not react appropriately to the higher security controls by vulnerabilities. The security concerns of IoT technology application presents a major challenge as it can cause disruption in IS security management. Recent attacks on IoT devices have demonstrated a need for new security solutions to secure this evolving technology particularly in its usage in SC [7].

Therefore, as a preliminary work towards revising the IS security management approach, this study aims to investigate the challenges associated in managing IS security in SC that are enabled by the use of IoT technology. In order to determine the challenges affecting the IS security management for IoT-enabled SC, a document analysis have been carried out. The analysis on the challenges is the initial part of the ongoing study to establish a framework for IS security management and an improved SC model driven by IoT technologies. This paper is structured as follows: The introduction of research on IS security management and IoT-enabled SCs as addressed in Section I. The literature review concerning the background of the study is discussed in Section II. The research method design is then explained in Section III, accompanied by discussions on the findings. Finally, the conclusion that includes limitations of the present work and suggestions for future work.

## 2. Literature Review

### *2.1. Impact of IoT implementation in Smart Cities towards information management*

Living in a digital age, including SC, in which most knowledge and information are now becoming extremely important. No one is able to deny that information and knowledge are valuable assets to be secured from unauthorized access including hackers, phishers, social engineers, viruses, and worms that endanger organizations from different angles via the use of intranet, extranet, and the internet [10]. Information systems (IS) are important in the operations of the organization. Hence, every organization associated in SC needs to identify the challenges which would impact there IS security management particularly with the adoption of IoT technology integrated with the IS.

The progression of information technology (IT) such as IoT and organizations' growing reliance on IT continually increases concerns regarding information security. Focusing on the concerns for IoT specifically, the security risks in IoT devices has risen and become critical over the last decade as studied by [11] and illustrated in Figure 1.

- *Issues in Information System Security Management in Smart Cities*

The management of IS from the implementation of IoT in SC faces cybercrimes issues such as information resources theft, data ownership, accessibility of information, and privacy issues, which can be arguably addressed by the establishment of information authorization and cyber security platforms [12, 13].

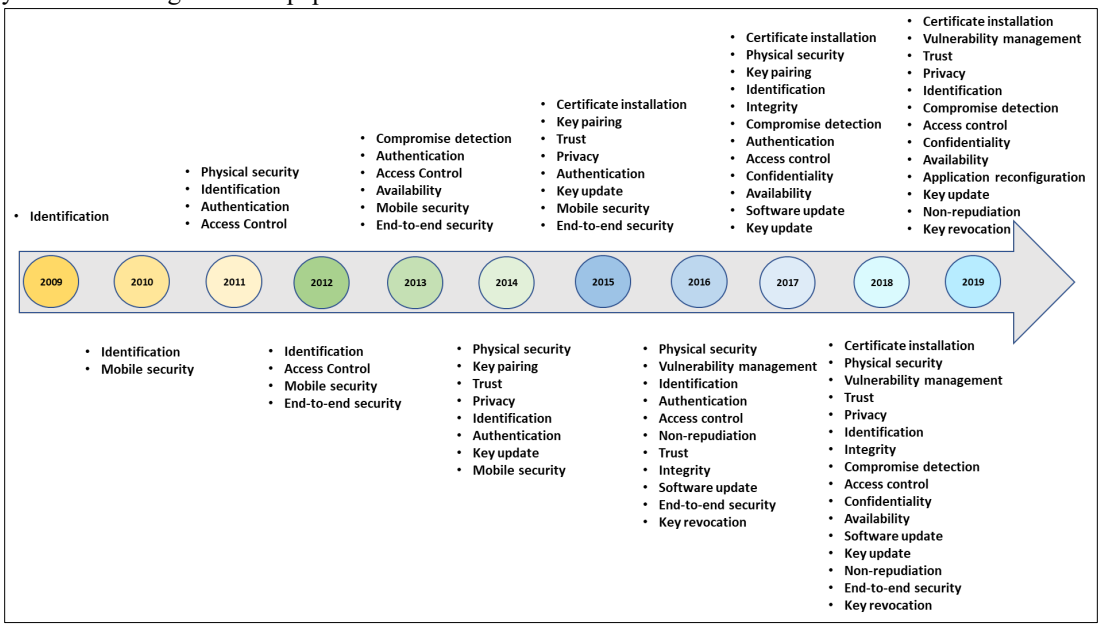


Figure 1: Evolution of Security Challenges in IoT Devices [11]

Other than that, an SC that adopts IoT technologies presents threats to the protection and privacy of both citizens and the government. This is because, security issues related to the information generated in an SC lead to the relationships and personal protection of citizens. Identity tracking, information leakage, spying, malicious programs, and inaccessibility to e-services are some critical issues being faced by organizations in SC that adopts IoT technology [4]. Furthermore, issues on scalability, mobility, deployment, interoperability with different technologies, legal, resources, and latency related to the utilization of IoT in SC must also be addressed. These issues particularly for essential services by organizations in SC must include protection against threats which would destroy or seriously harm the operating capacity of a community, from manufacturing sites to vital services, including access to power, gas, and water [4].

Table 1 presents a summarized collection of issues identified from existing relevant reports that are categorized according to basic security aspects in managing the IS security in SC.

Table 1: Issues in Information System Security Management in Smart Cities

| Categories | Issues | Sources |
|---|---|---|
| Smart City Administrative | There is a lack of clear strategy plan for SC development and a decentralized regulations and legislations. The vertical nature of city system is causing siloes in its operation. Furthermore, the urban authority is unwilling to invest on data transmission process and ICT infrastructure upgrades. | [14,15] |
| Information Privacy | An interdependencies among systems in SC increases vulnerabilities and privacy issues. There is a high potential risk of confidential information leaked from citizens access to the services through the use of multiple devices, various networks and systems. | [15,16] |
| Information Confidentiality | Unauthorized access to personal information is due to access control vulnerabilities. Confidential of information is where no one can access to information which is belong to specific individual. The limitation of individual access needs to be identified to certain information via username and password credentials. | [16–18] |
| Potential attack | Cyber-attack issues due to ineffective cybersecurity evaluation, unclear security features among connected devices, poor security functionality execution, obsolete and ineffective encryption methods, inadequate emergency response plans, massive and complicated attack surfaces, software installation that was not updated, insecure legacy systems, and Denial of Service (DoS). Furthermore, there are also weaknesses in the data relocation, physical effects of cyber-attacks, huge volumes of data gathering and storage using cloud technology, and manipulation of data by hackers. | [4,5,17] |
| System Integration | Integration of multiple applications with different datasets poses threats to the cyber vulnerabilities. Poor integration structure and rigid ICT infrastructure to handle multiple data types impact access to emerging technologies, complicates technology acquisition and relocation. The SC interoperability mechanism also often enables information to be interpreted and distributed via the infrastructure which are prone to cyber-attacks and threaten the integrity of information. | [4,14,15,19] |
| Citizen's Acceptance | Poor citizen engagement because of less trust and poor level of awareness regarding the commercialization of new concepts, and the improvement of technology. | [14,17] |
| Information Management | IoT will produce a large amount of data and it will result in data management challenges while recognizing, processing, and handling the data. | [4,20] |

In an SC plan, privacy would become a fundamental role. The study by [16] proposes the definition of privacy based on control of data disclosure, and incorporates mechanisms to safeguard the confidentiality of individuals' information while sharing their data. Personal information extraction (acquiring and covering data sources belonging to someone), privacy-preserving data mining (partnership among organizations and getting information without exposing all details), confidentiality of place, and Radio Frequency Identification (RFID) are examples of such approaches [4].

Furthermore, SC is a complex interconnected structure where a single weakness can have a major effect on the safety of its citizen, for example, to connect to the internet and convert existing public transport to potential smart transport systems, which would be possible for an intruder to link to the electric power grid. False alarm is one of the threats that can also be introduced while attackers modify traffic lights and controllers. Thus, practical solutions are essential to overcome this incident. Otherwise, the community will not trust SC projects, and they will not be sustainable. Security features like the capability to protect email, web browsing, and other transactions depend on the devices used in the IoT technology. The efficiency of secure implementation among all of these characteristics in an SC is required for these devices [4].

Due to this, information management manages a huge volume of data, for example, data from mobile phones which will help achieve some targets for SC. To construct a variety of urban applications, smartphone data can be used. During an analysis of transport, mobile phone data can be used to estimate the volume of road traffic and transport requirements. In combination with taxis' Global Positioning System data, real-time information from mobile phones on the origins of visitors could better facilitate transport resources [4].

On the other hand, compliance to the criteria of IS security management in SC-enabled IoT is a warranty that IS is well protected. Auditing is a verification procedure, including inspection or review of a process or quality system. Besides, some audit functionalities monitor completed remedial actions. Therefore, the processes used for auditing and the IoT device for automated auditing with little human interference need to be incorporated [21]. In addition, digital forensic is also a method of computer evidence preservation, recognition, retrieval, and recording that can be used in court. Digital devices, consisting of computers, cell phones, server, or network, will identify the facts. To solve complex digital cases, the forensic community will select the best strategy [22].

One of the existing approaches to manage IS security is International Standard ISO/IEC 27001 (Information technology-Security techniques-Information security management systems-Requirements [23,24]. ISO/IEC 27001 is complemented by the implementation guideline within ISO 27002. This standard is imposed by the Information Security Policies as mandatory for information security management. In an SC environment, security management of the information system plays an important role in ensuring that protected information is obtained and transmitted by adopting IoT technology.

Governance for information security can be identified as a process which deals with procedures and methods for monitoring information availability, accessibility, reliability, and safety and compliance with government policies [25,26]. The vital issue is it requires full commitment and support from the top management of the organization for the execution of information security management [27]. In an SC, the systems will be implemented in a single platform to aggregate data and manage SC initiatives. All organizations and stakeholders involved in SC organizations must play their role in controlling information security management [28], which includes strategies, procedures, and organizational processes that guarantee the protection of the organization's resources, the consistency and reliability of documents, and organizational alignment with the requirements of management [6].

Besides that, the organization also needs to consider the development of Information Security Policy as a subset under IS security governance. Information Security Policy relates to the document(s) governing human activities concerning information security or expressing the information security goals of the organization [29]. This policy will ensure the security of information assets and information technology with a particular process to facilitate the goals and objectives of an organization. It consists of strategies, processes, and technological measures used to avoid unauthorized access to IS, modification, stealing, or physical harm [6,10].

Other than that, the selection of vendors in developing and implementing of SC also needs to be highlighted. The vendor appointed must be independent in order to protect organizations against monopolies, push for standardization, and protect competitiveness between technology vendors [30–32]. The vendor selection process includes designing a plan for contract negotiation. Organizations want to cooperate with vendors, because they can all achieve the same objectives and goals. Good negotiation of contract means that both parties are aiming for positive impacts that benefit both sides in any aspect while also reaching a fair and equal agreement [31].

### *2.2. Internet of Things (IoT)-Enabled Smart City Information System Security Management*

IoT is a global IT infrastructure that allows advanced networks to interconnect objects depending on existing and evolving interoperable technologies of information and communication [33]. The IoT vision lets people and objects to be linked with anything and anyone, anytime, and anywhere ideally through any networks and services. The foundation of the future IoT will be recognition technologies, for instance RFID and related devices [34]. The IoT is a key-emerging technology that sets the stage for industrial production systems of the next era. Smart industries will constitute self-organizing production systems that include across organization borders, as well as manage everything with regard to availability and utilization [35]. Furthermore, IoT provides multiple services which are of great interest to SC, not restricted to increasing the quality life, but also leveraging urban administration by reducing operational costs [36].

- *Security Management Requirements for Internet of Things (IoT)-enabled Smart City Information System*

From the security perspective, IoT protection aims toward protecting privacy and confidentiality, and guarantee the safety of IoT users, infrastructures, information, and devices, and ensure the readiness of IoT ecosystem services [37]. For IoT technology in SC, ensuring data protection from unauthorized access is the most difficult. Different private information that must be detected, authenticated, and controlled at their access levels will be obtained by IoT devices by permitting only authorized parties to monitor and access data. A comprehensive cyber security for IoT system industries that addresses multiple security and privacy risks at all levels is needed to tackle these security and privacy risks. Furthermore, the protection and privacy sides of smart systems and smart products must be protected throughout the lifetime [35].

A study by [38] has recognized that high levels of IoT protection specifications include:

i. *User identification* by validating clients prior to giving the device permission.
ii. *Secure storage* of complex information contained in the system requires confidentiality and integrity.
iii. *Identity management* by recognizing individuals/things in a system and monitoring the access to services within this system through correlating access privileges and limitations per identity created.
iv. *Secure data communication*, which contains authenticating, maintaining the security, and credibility of linked information, avoiding a message transaction from being repudiated, and preserving the privacy of the users involved.
v. *Availability* refers to making sure that illegal individuals or systems cannot be used as authorized users.
vi. *Secure network access*, providing network connectivity and service access only if the device is enabled.
vii. *Secure content* by Digital Rights Management (DRM) that safeguards the rights of the digital information used in the system.
viii. *Secure execution environment* is designed toward protection, which is a process to safeguard the operating environment, managed-code, and built to protect from deviation reporting.
ix. *Tamper resistance*, even when the device falls into the hands of hostile parties, refers to the ability to uphold certain protection standards and can be physically or logically checked.

Another study, which focuses on the influencing components for IoT security, has also raised areas to be highlighted [34]:

i. *Authorization* in access control of devices and services for the purpose of secrecy and integrity of data.
ii. *Authentication* concerning service users and system users' authentication which aims for authentication and accountability.
iii. *Identity Management* in management of identities [44], pseudonyms, and associated access policies for the protection of users and privacy of services.
iv. *Key exchange* and management by cryptographic key exchange for the purpose of communication confidentiality and integrity; and
v. *Trust management and reputation* by degree of confidence in service and gathering user credibility ratings to maintain trust and reputation in services.

- *Issues in Internet of Things (IoT)-enabled Smart City Information System Security Management*

Related to the complexity of the devices and applications, as well as the size or volume of devices on the network, the implementation of protection mechanisms is more complicated under IoT conditions than in conventional operations. Physical pairing, heterogeneity, limited resources, confidentiality, large scale, trust management, and lack of preparation for protection become the challenges in applying IoT security management [7]. Resource constraints generally include restricted processing resources, power supply, and memory space. These characteristics are hard to make use in many conventional safety solutions of IoT, with the broadly applied public key scheme and IP-based protection solution. It is also simpler for attackers to hack IoT devices than traditional computers due to inadequate IoT protection architecture [7].

The primary feature of an urban IoT infrastructure is its ability to collaborate among multiple technologies with current connectivity infrastructures to facilitate a progressive assessment of IoT, integrate some devices, and recognize new functionalities and facilities. Some other fundamental parts are how to make the information gathered by IoT devices accessible to stakeholders and citizens, to enhance the sensitivity of stakeholders to urban difficulties, and to encourage awareness and public involvement of citizens [39].

With the massive rise of IoT devices, the information gathered by these devices will introduce different obstacles on how to evaluate large volume of information. It would not be advantageous for someone to obtain the information until there is a way to interpret and understand it [40]. In addition, International Data Corporation (IDC) has projected that by 2025, the total amount of data generated by IoT devices will be around 180 zettabytes. This amazing progress is either from the number of data generation devices or from various sensors in each system [41] as shown in Figure 2.

In recent years, the number of security threats directly linked to IoT devices has increased, such as privacy attack, data alteration, protocol and session hijacking, data interruption, data collection, message replay, and data leakage [42], which are caused by unreliable authentication, inadequate authorization, and lack of configuration for protection. Besides that, Threatpost expects that more than 2 million intelligent devices are open to hackers with no safety solution. Several cyber-attacks, such as the Malware and Ransomware, affect the safety of smart devices [43]. These IoT security issues will result in difficulty of managing the information through the IS in SC environment, which involves IoT technology.

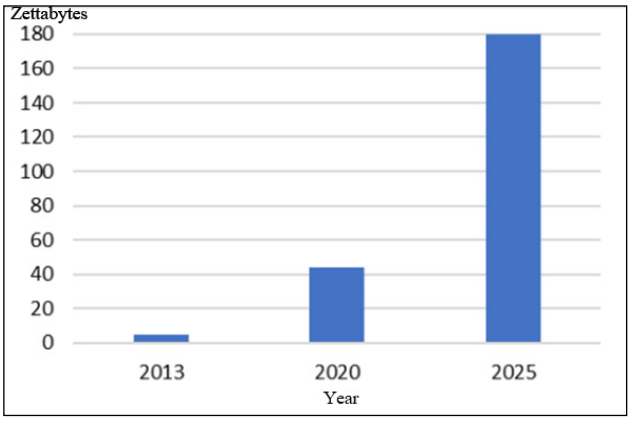


Figure 2: Expected Data Generated by IoT Devices in Zettabytes [41]

From another perspective of information safety, none of the smart devices, such as smart home apps, are insignificant as each reflects a possible attack avenue for hackers to exploit and get inside, and access the environment within a home network. Based on available industrial data, 11 smart devices, including accessories, are housed on average smart homes in the United States with an average of two devices per home. The most popular smart home devices in the US are smartphones (91 percent), smart TVs (73 percent), and tablets (72 percent) [3]. Smart TVs with 24/7 access and internet connectivity are becoming normal. It is possible to connect almost any smart home appliances to the network. Any internet-connected standalone computers that can be controlled and/or operated from a remote place are called IoT devices [44]. This development brings significant advantages and various savings, but in contrast to this, there are multiple threats in the aspects of private information safeguard, electronic commerce, and safety of infrastructure.

When IoT becomes a core aspect of the future internet and for large-scale use, most systems present a requirement to handle confidence and safety roles adequately. New threats to privacy, confidence, and reliability have been established. New threats to privacy, trust, and reliability have been defined, including providing confidence and information quality of shared information models to encourage reuse throughout many applications, ensuring secure information exchange among IoT devices and users, and providing vulnerable devices with security features [45]. As IoT makes it easy to access large quantities of information through remote access mechanisms, IoT privacy security has become more difficult. Hackers do not need to physically exist to collect data, but can perform secretly at a very low risk [34].

Table 2 presents a summary of issues identified for managing the IS security in IoT-enabled SC that are categorized according to the IoT security issues discussed in previous studies.

Some scholars recognize IoT security challenges of user privacy, authentication, authorization, and trust management [42]. The protection of the baseline must be stable and the security policy must be built for long device life span (more than 20 years)

[34]. The major security challenges are found to be availability (avoiding DoS), failure prevention (safeguarding integrity), and confidentiality across information, data, and device design [35] through more conditions, such as authentication, confidentiality, and access control [56]. In contrast, a study by [38] considers the safety conditions, such as resistance to incidents, data certification, gaining access to control, and confidentiality.

Table 2: Issues for IoT-Enabled Smart Cities Information System Security Management

| Categories | Issues | Sources |
|---|---|---|
| Access Control | To support identification entities and guarantee users and things to access permission to interact with the system. It also manages an immense volume of data transmitted in a commonly recognized representation. | [34,46,47] |
| Authentication | A vulnerability during integration between two or more information systems or parties. The authentication process among each other is needed for validating process. | [34,46,48] |
| Authorization | Device authentication which uses weak or default passwords allows attackers the opportunities for information manipulation and physical device harm. The devices can only obtain access to facilities or applications after precisely presenting their identities. | [34,46–48] |
| Privacy | Users demand that their personal data related to their movements, behaviors, and interactions with other individuals be protected. | [46,49,50] |
| Confidentiality | To ensure a process for an end-to-end verification of integrity in order to make the system more robust to malicious attacks. | [38,46,49] |
| Policy Enforcement | The policy enforcement mechanisms is to protect the organizations information. Thus, a cross domain policy implementation is important to manage the appropriate policy implementation in the increasing connections and interactions between domains. | [24,26,34] |
| Resources | Limited capacity in IoT devices for processing and storage due to its small and lightweight characteristics that make them operate on lower energy. | [48,51] |
| Big Data | The volume, speed, and diversity of data involved makes it difficult to store and analyze in order to prepare valuable information in real time. | [32,48] |
| Secure Communications | Insufficient protection of IoT devices, result in less guarantee of information system being secured. Most IoT devices send out data in plain text format without encryption that makes it vulnerable as targets to various network attacks. | [38,48] |
| System Resilience | Less capability of the application to react to unexpected incidents. If one IoT device is attacked, there are possibilities of other devices or another network points to be attacked. | [48,52] |
| Complex System | The integration of multiple IoT devices involving the technology, users, collaboration and interfaces creates a complex system. The concern is primarily in ensuring the interaction process among the IoT devices is complete, especially concerning memory, power, and time constraints. As more devices, users, collaboration, and interfaces involved will pose greater risk of security breaches. | [4,48,51] |
| Trust | Lack of citizens' confidence and trust in the security of user data and privacy have an impact on the decreased IoT adoption rate. However, acceptance on IoT technology utilization is critical in the success of IoT. The principle of integrity must be upheld to ensure the protection of unauthorized modifications to data, software and hardware components. | [34,42,48,53] |
| Risks | There are increasing risks to personal data privacy with the increasing use of IoT devices, which requires more protection. The risk involves the complex authentication processes in ensuring the users' privacy, the lack of organization's knowledge and experience in the IoT security, insufficient data encryption, and a complex information system with integration of more devices, users, communications and interface. | [7,34,54] |
| System Integration | Organizations may use multiple standards to strengthen their applications involved in the system integration. With various data sources and heterogeneous devices, it is important to have standardization. This is important for applications involved in inter-organizational and multiple system boundaries. | [24,45,55] |
| Auditing | The IoT security auditing is performed manually, slowly, and is not flexible for the IoT cases, and an auditing challenge. | [21,22] |
| Digital Forensic | The identification, collection, and protection in IoT system are challenging due to device being built to operate passively and autonomously. Most IoT devices do not store metadata, which make the provenance of facts an investigator's challenge. In a technological perspective, privacy is a main issue to address when analyzing and correlating collected data, especially as inherent personal information is collected by many IoT sensors. Attack of deficit attribution, where an important outcome of any forensic investigation is to recognize illegal criminals in the event of an incident. | [18,21,22] |

In the aspect of IoT organization, there are multiple threats that can impact it, such as attacks on different communication networks, physical threats, denial of service, and identity manipulation. The inherent complexity of IoT, where various distributed entities will share information in different contexts within one another, will lead to more complications in the design and implementation of efficient, interoperable, and scalable protection mechanisms [57]. Besides that, heterogeneity is one of the issues that will impact the protection of the IoT. The protocol and network security services which need to be introduced in the IoT have a significant effect on it. Constrained devices will communicate either immediately or via gateways with different heterogeneous devices, which will also affect identity management [57].

- *Authentication and Identity Management*

Authentication and Identity Management are a combination of procedures and technology designed to maintain and secure access to information and resources while maintaining profiles of items. Authentication is the guarantee that no one, excluding the person with authentication like user ID and password, can access the information. Identity management recognizes objects uniquely, and authentication requires validating the establishment of identification between two interacting parties. As multiple users and devices have to be authenticated by trusted services, it is important to consider how to handle identity authentication in the IoT [34]. Identity management in IoT provides both challenges and potentials of improving security [53]. The underlying process and individuality of objects are different and the most critical elements of this obstacle. Identity management specifies the actual 'identity' scope, and certain processes must also be established to achieve universal authentication. It would not be possible to ensure that the data flow generated by other entities comprises of what is intended to be included without authentication. Authorization is another significant factor connected to authentication. If there is no access control at all, anything that is neither feasible nor practical will be accessed by everybody. In reality, a major challenge to privacy is the data continuous stream created by billions of information-generating entities [57].

- *Authorization and Access Control*

Authorization makes it possible to decide if the person or object is authorized to have the access to information or resources until it is identified. Control of access means controlling through granting or refusing access to services according to a large variety of requirements. Authorization is commonly adopted by the use of controls for entry. In setting up link between a number of devices and services, authorization and access control are essential and interdependent [34,47]. In order to accommodate the different authorization and use models needed by users, IoT needs a variety of access controls. The complexity and variety of devices that need access control would require the creation of new flexible schemes. In IoT-based systems, cryptographic technique is also necessary to allow data to be stored and exchanged by means of security without the information content being available to other parties [58].

- *Trust Management*

Toward the aim of understanding the challenges in IoT, the trust and reputation of the system also need to be emphasized. The pre-defined trust management criteria consist of trustworthiness, adaptability, usability, privacy, accuracy, efficiency, uniformity, comprehension, and generality [59]. There are three types of trust as follows [56]:

i. Trust proportion is where the ratio of efficient transmission of packets between nodes to all forwarded packets at a given time scale occurs.
ii. Trust in communication is the scenario when the distance between the source and the destination node is small, and relies on the direct transfer of the packet. If the number of packet interactions is not sufficiently high to represent the trust between nodes, the mechanism will be efficient by relying on and seen among common neighbors between senders and receivers based on their recommendations.
iii. Energy trust is an estimation of the energy of the transmitted data to receive or forward messages, either directly or through intermediate nodes, among destination nodes.

Study by [84] proposes an IoT trust management mechanism that can determine a node's trust level from its past behaviors in various cooperative services. The main objective of this approach is to facilitate collaboration by using a decentralized strategy in a heterogeneous IoT architecture due to the varying capabilities of nodes. In order to update trust values, two models are taken into account; first-hand information (i.e. by doing observations and own experiences) and second-hand information (i.e. indirect experiences and observations recorded by neighboring nodes). At the same time, trust management system involves four phases which include: (i) Collecting information on the trustworthiness of accessible nodes; (ii) Creating a supportive service with the nodes requested; (iii) Improving previous activities by updating itself to enhance ongoing development; and (iv) Determining each node a performance assessment rating during the learning phase after each interaction.

- *Privacy*

A key-changed shared authentication scheme for WSN and RFID systems is provided with an emphasis on privacy security in IoT [62]. Such a protocol combines the tag and the reader with a random number generator and incorporates the one-way hash feature, the key real-time refresh, and the key backup as mechanisms to minimize the possibility of replay, duplication, denial of service, spoofing, and tag tracking. The Privacy Preserving Data Mining (PPDM) methods are designed to minimize the risk of sensitive data exposure and the analysis of sensitive information. In such a case, the issue of user privacy knowledge is raised, implying a method of privacy protection that allows users to estimate the risks of sharing sensitive data. It also aims to establish a comprehensive technique for detecting sensitivity, and to measure the data's privacy content. In addition, the evaluation of data protection criteria, given by various sources, describes a layered IoT architecture to estimate both the quality of the data and the level of security and privacy.

## 3. Method

Document analysis method was implemented in this study. The key objective of this study is to discover the challenges of managing IS security in SC enabled by IoT through analysis using the guidelines provided by [60]. To fulfil the task, the following steps were taken:

### *3.1. Selection of Documents*

A broad search was conducted on published or unpublished documents about IS security management and IoT security management to find reports on challenges in IS security management for IoT-enabled SC, and to find documents which would specifically address the questions of the study. The documents comprise of journals, proceedings, research theses, governments' official documents, established reports, paperwork, and official web portals. A total of 90 documents was chosen for the collection after all the searches were carried out.

### 3.2. Searching criteria

Queries were done on online databases as well as e-journal repositories, such as Web of Science, Scopus, Science Direct, IEEE, ACM Digital Library, and Springer Link. Besides, the governments' web portals of selected SCs and news articles were also explored to gain perspectives and viewpoints on the topic being studied. The searching process used open search engines, such as Google Scholar, Google, and research gates. Keywords such as "information system security", "Internet of Things security", "smart cities challenges", and "cybersecurity" were used during the searching process. The search included leading journals in the fields of information security and information systems, without constraints on the year of publication, i.e., between 2010 and 2020.

### 3.3. Data Analysis

The 90 collected articles were then analyzed and interpreted using document analysis method [61]. The analysis process included identification and coding, as well as analysis and interpretation of data into categories. Coding was conducted during the identification process by examining data into meaningful and unique information units. Subsequently, themes were created by iterative comparison to reflect the underlying meaning of data. For organizing the content into similar categories, the specified categories were used. Throughout the research, these processes were continuously carried out to meet the challenges that ensure effective management of IS security in an IoT-enabled SC. This produces some insights into the challenges that impact both public and private organizations IS security management for IoT-enabled SC. As a result, a set of challenges in five aspects have been identified. The aspects include governance, integrity, interoperability, personalization, and self-organizing.

## 4. Result and Discussion

Based on IS and IoT security management scenario, challenges on IS security management in SC-enabled IoT have been identified. The comparison criteria were based on the frequent issues discussed in previous studies. The key challenge was to ensure that the functionality of IoT technology working without human intervention met with the safety requirements. Failure to meet these criteria would result in the challenge of protecting IS from cyber criminals and cyber hackers.

In IoT-enabled SC, we identified challenges explicitly related to IS Security Management. We revealed 18 challenges classified into (1) governance, (2) integrity, (3) interoperability, (4) personalization, and (5) self-organizing. A description of the 18 challenges related to IS security management in IoT-enabled SC is presented in Table 3.

Information security focuses on confidentiality, integrity, and accessibility of digital information assets, such as data, information, knowledge, and relevant IT assets (hardware, software, and networks). Meanwhile, incident in information security is a single or sequence of unwanted or unexpected incidents in information security that has a significant risk of disrupting the business process and threatening the security of information [28]. Managing IS security in SC ecosystem by using IoT technologies must be concentrated on wholly integrated applications rather than stressing on in a single application. The main criterion that is important to emphasize SC managerial is the level of IS security, whereby the level of IS security among organizations is integrated by setting it at different levels. For instance, certain organizations have been set up as low level of safety, and other organizations have setup as high-level security based on their needs [19].

Table 3: Information System Security Management for IoT-enabled Smart City Challenges

| Aspect | Challenges | IS Security | IoT Security |
|---|---|---|---|
| Governance | Formation and management of security standards / policies for IS | [6,14,24–27,29] | [14,45] |
| | Coordination of multiple stakeholders and organization | [24,28,58, 61] | [14,39] |
| | Quality assurance | [6,62–64] | [56] |
| | Citizens' involvement | [14,50] | [39,54] |
| Integrity | Information security | [6,24,49] | [34,38,42,65] |
| | Information privacy | [6,15,16,24, 49,63] | [34,37,45,65] |
| | Existing IS architecture | [14,61,66] | [7,39,65] |
| | Continuous cyber-attacks | [6,10,12,13, 24,63,67] | [42,48,65] |
| Interoperability | Readiness of organization | [6,58,68] | [14,45] |
| | Interoperability implementation | [15,19] | [45,65] |
| | Secure communication | [4,6,62] | [38,48] |
| Personalization | Confidentiality | [4,17] | [37,56,65] |
| | Identity management | [17,69] | [17,35,38,42, 48,54,56,70–72] |
| | Trust and system reputation | [4,14,73] | [42,45,57,68, 70,74] |
| Self-Organizing | Threats/Risk management | [4,11,75] | [35,54,71,72] |
| | Lack of smarter security system | [24] | [71] |
| | Availability | [17,25,26] | [17,37,48,63, 70,71,76] |
| | Reliability | [14,69] | [45,77] |

Besides that, the SC characteristics, which will be enabled by IoT, are personalization and self-organizing. The personalization component is the individual provision of information, especially based on individual profiles and needs [81]. Self-organization, meanwhile, is a single concept of integrating the whole thing and can be defined as connecting anything to the internet, whether it is a computerized device system with no human-to-human or human-to-computer communication required [69]. One of the IoT elements is to gather and manage individual information automatically in real time. IoT typically consists of unlimited quantities of devices, individuals, and services that link and share information from various resources. Due to additional devices attached to each other in IoT ecosystems and the universal usage, the security and privacy issues come to be the key concerns.

The discussion on the challenges for each aspect is presented below:

### *4.1. Governance*

The leadership and administration in the implementation of an SC can affect security issues. The SC must have all the means to maintain infrastructure and management issues, but weaknesses and frauds can result from inappropriate implementation. Therefore, it is important that the governance of IS security management within the SC is improved by taking into account the integration and exchange of information between different stakeholders, and by carrying out information security assessments. As it indirectly allows organizations to make effective and in-time decisions, the security level of the IS using IoT equipment must be maintained.

Information System (IS) security standard/policy development and management in governance need to be available and organized in the execution of collaboration and information sharing in the SC-enabled IoT [62,78]. Multiple IS incorporation by the use of different IoT devices enables the sharing of information in an SC. This condition will result in chances of IS security risks. The possible risks of cyber-attacks, such as distributed denial-of-service (DDoS), on public infrastructure will rise once devices are connected extensively to generate substantially huge volumes of information [79].

Besides that, coordinating between different stakeholders and organizations due to security management procedure in IS collaboration stays low [64,80]. There is an inadequate standard in the supervision of many stakeholders and no single standard is completely set in the governance of IS protection related to the acceptance, process management and dissemination of information through the use of IoT in SC [58]. In governance, the most comparable activities in IS integration in SC should be correctly described. The governance elements must include strategies, policies, processes and legislation, and accountability. The direction of an organization will be defined by strategies and policies, while processes and legislation will detail who, what, and how. Accountability explains the positions and responsibilities of stakeholders [62]. For example, in the health industry, it is important for medical personnel to safeguard patients' details. Otherwise, the data is open vulnerably, and worse, exploits the responsibility of the staffs for it, so they should be kept responsible for this to prevent future abuses [52,81].

Security measurement for the exchange of information, transmission, cooperation, decision-making, and execution of information exchange during the phase of IS integration at SC must be well-established for IS quality assurance [6,62]. Secure management would therefore require safe monitoring by the coordinator, where the function of the coordinator is to add and remove the IS involved in integration [52,81]. Quality assurance shall ensure that all decisions, processes, and activities remain in accordance with requirements to prevent service risks prior to their occurrence [82]. In order to ensure compliance with information security policies, standards and procedures, rules, regulations or contractual requirements of each company, the implementation of auditing and digital forensic processes is therefore critical [10].

Digital forensic is becoming more critical as an investigative activity for tracing and analyzing criminal and fraudulent activities. Digital forensic is all about cybercrimes, mobile forensics, investigating methods, and analyzing illegal incidents with aims to gather digital evidences. Information will be obtained for law enforcement purposes. Digital forensic may be aided by Intrusion Detection and Prevention Systems (IDPS), as it may confirm to be an important instrument, where its purpose is to conduct initial discovery, track malicious behaviors, and likely avoid further major harm to protected systems. An IDPS is therefore a very valuable instrument for the processing and interpretation of forensic evidence, which can be used for the purposes of a legal proceeding [31].

Other than that, involvement of citizens in SC ecosystem is needed to sustain the IoT usage. A low rate of citizen participation is due to lack of confidence and poor IoT knowledge levels. In order to address this problem, people need to recognize that IoT devices and related services can secure their personal information and help build a sense of empowerment [14,48]. Another important security and privacy measure is the understanding of cyber security and privacy. This is because some citizens do not understand this form of event and the negative impacts it can have, and are thus not in a condition to make decisions on the effect it can have on their privacy standards [83]. Cyber security awareness can begin at early levels, such as kindergartens and schools. Teachers or academic staffs can educate by teaching the implications and risks of cyber incidents. Teachers should also teach what is new, thereby ensuring a better image of the level of knowledge at personal and community levels [31]. Furthermore, it is also important to take social aspects into account. Thus, the "smartness" of a city relies heavily on the participation of citizens in SC projects via numerous communication channels comprising of online portals, social media platforms, and smartphones. In order to share experience and expertise, SC requires people to be actively linked in public locations, public transports, and at homes [4].

### *4.2. Integrity*

Each part in SC, targeted and hacked in IS via cyber-attacks, would breach the integrity of information sharing and the privacy of information of users [82]. The definition of integrity is to ensure that unauthorized changes to system components are protected. Measurement to protect the content, authenticity, and continuity of the message must be taken [52]. There is no

unauthorized alteration of information by permitted or unauthorized personnel, and the information is internally and externally consistent [65, 84].

The weakness of IS security management in SC via the use of IoT will allow unauthorized users to retrieve information [58]. It can cause unauthorized data alterations, damage to information, and loss of information. Thus, the guarantee of information will be questioned by people including the impacts. As a consequence, the security of details that will affect the day-to-day activities of a company is not guaranteed [63, 73]. Information with credibility is reliable information that helps the organization in making the correct decision.

Other than that, the process of preserving data and information confidentiality, authenticating, identifying data, and controlling user access will be the subject of data protection. Theft of identities and phishing are some of the threats to information security, i.e., attempts to trace the misuse of one's financial information, duplication of user accounts, and fake sales or hacker promotions, which can result in data and information being disclosed, updated, and destroyed. Consequently, the integrity of information and data will decrease significantly, and users would lose confidence [65, 73]. Another example is, in medical applications, the node should be able to confirm that the data is sent from a proven trust center. Therefore, by changing the unknown key, the network node and coordinator for all data will make measurements to the Message Verification Code (MAC). Accurate MAC code measurement guarantees the network coordinator that a trustworthy node executes [85].

In addition to that, privacy concerns often affect the integrity of information. Privacy is the right to monitor and protect a single individual's private information. Security must guarantee that without the permission of the owner, none of the single bit of information obtained for a particular user can be shared with others. One of the most critical steps to protect privacy is the creation of rules/policies that have the capability to obtain confidential information in order to protect privacy [52]. Private information is collected in the IoT-enabled SC environment, where various devices are part of public services, for the users to decide with whom the information can be distributed [65,86]. Processing confidential information and the right of users to disclose information on the internet or social media on digital networks are the focal points of this privacy. SCs are exposed to privacy leaks and the collection of information by hackers, particularly, when private information is collected, distributed, and processed. Revealed privacy in SCs may include the identity of a user, venue, transportation movement, health status in healthcare, intelligent surveillance lifestyle, and home and community smart energy. It would be a big mistake to expose this privacy-sensitive data to untrusted or unauthorized people in the real world and cyberspace [73].

Compared to the SC setting that requires IS integrated architecture, some other elements of the constraints of the current IS architecture are linked to initial implementation in silos. The design is divided into software, hardware, and processes [64]. The software architecture is critical for delivering connectivity and allowing IoT devices to share resources between integrated organizations. The hardware/network architecture must be capable in supporting the IoT-critically disseminated computing environment. In an organization, the use of IoT can impact existing business processes. Therefore, to help the innovation in computing and technology, there is a requirement to integrate IoT technology in organizational activities.

Furthermore, a big data project with massive amount of data will arrive in real time. The number, velocity, and variety of data can complicate the process of storage and analysis used to produce important information [48]. Increasing the amount of IoT devices used by SC in IS will provide hackers with opportunities for information security risks as many SC-related devices have low levels of security. IS security monitoring vulnerabilities present a threat to cyber-attacks exposing data to leakage [63, 65, 75] and access breaches. The lack of preparation to handle current cyber-attack threats would result in information being destroyed and lost. Cyber-attack is a security threat that is able to affect the expense of mitigating organizations [75]. Thus, system stability in terms of the system's ability is to react without getting worse because of unexpected attacks. The device must also be capable of protecting other network points from any attacks if one IoT computer is hacked. Therefore, mechanisms to ensure the protection, availability, accuracy, and integrity of the information system must be established during the sharing and processing of information in the SC ecosystem. One of them is the Intrusion Detection and Prevention System (IDPS) which is a computer or software program designed for network or system monitoring. It recognizes weaknesses, reports malicious attacks, and imposes protective methods to keep up with the progress of computer-related crimes via multiple response techniques [87].

### *4.3. Interoperability*

Interoperability is a mechanism for sharing data and using knowledge that combines two or more systems or elements. Interoperability requirements make the system integration process vague, inadequate, and complicated, if not difficult, to execute [86, 88].

The vulnerabilities in IS protection make it impossible to be secure in the management of information exchanges, especially with a view to promote interoperability in the interaction and coordination processes of different IS that would allow services to citizens [24, 54]. Organizations' preparedness to use IoT in organizational activities is still poor and must be strengthened. An automated connection is required between various devices, facilities, and programs. The use of various technologies provided by IS providers would contribute to the need to separately manage the device. Security risks to information inside the SC would be indirectly revealed in the implementation of interoperability between organizations by using different levels of IS protection [80, 89].

Therefore, it is difficult to ensure that the interaction process between IoT devices is complete in each organization that includes multiple devices, especially with regard to memory, power, and time constraints [48]. So, before organizations are ready to be integrated, the requirements for the implementation of interoperability should take into account different levels of IS protection set by the company. This is to ensure that the integrated system's security is maintained [15, 19, 45].

Other than that, secure communication is another critical factor that must be highlighted during integration [65]. It will guarantee the security of authentication, confidentiality, and integrity of the linked data. It also prevents a message exchange from being repudiated, and preserves the identity of the users involved. Moreover, it is insufficient to protect IoT devices solely to ensure that the IoT system is completely protected [38,48].

### *4.4. Personalization*

Personalization services are delivered according to individual profiles and preferences in a unique and precise way [79]. Confidentiality and privacy prevent data to go against unauthorized access where data indicates the security of an exposure to sensitive data that is deemed to be the critical issue. For example, in a medical context, sensitive and personal information about a patient's well-being is required and relied on to be transmitted, so the patient's data must be shielded from unauthorized access that may be harmful to the safety of the patient. Encryption will provide this sensitive data with greater security by using a mutual key to secure communication [52]. In order to make life safer and easier, the IS used every day will automatically collect personal information in real time, which means that IS can also monitor everyday life activities. If the IoT system control is lost or stolen, it will be a serious potential security concern [74]. In comparison, in the internet world, there is no chance for attackers to access the information if individuals do not supply the necessary details.

One aspect that needs to be highlighted in information protection is identity management. The access control restrictions for approved users are also not adequately implemented. Consequently, attackers may take advantage of these vulnerabilities to retrieve unauthorized features and/or information, such as accessing user accounts, watching confidential files, manipulating user information, and modifying access privileges [17,69]. Moreover, in the functions of applications, authentication and session management are still not properly implemented. Cyber-attacks affect IS authentication by enabling third parties to manipulate the original data to make it unreliable. Attackers can modify or manipulate other weaknesses via passwords, keys, and session tokens [17].

Besides that, trust and device credibility are essential aspects of using IoT to manage IS security. Trust ensures that information and resources are fully and confidentially accessed by users and IoT devices. Competent data collection, powerful data combination and mining, and enhanced user confidentiality are included in trust management. The present challenges are determining how trust is established between IoT devices, and determining the trustworthiness of a user in the use of IoT devices [17]. In IoT, consideration of two aspects of trust must be emphasized, consisting of trust concerning the interconnection among entities and trust in the system from the clients' viewpoint [57].

Personalization relies on the usage of private information, and in this IoT feature, protection and privacy issues are therefore major concerns. Organizations need to be fulfilled with security requirements, such as identity protection, privacy, data access control, precise authentication procedures, and trustworthy identity to resolve this.

### *4.5. Self-Organizing*

Self-organizing is the administration of automated Machine-to-Machine (M2M) acceptance, processing, and distribution of information without human intervention [24,58,90]. In other words, in order to generate customer-oriented output that continuously operates to sustain itself, computers will function independently or coordinate with humans. The machines are thus autonomous entities that can gather and interpret information and provide guidance on the basis of research [90].

One aspect that needs to be highlighted in self-organizing is risk management. Risk is an essential aspect of the management of IS security in IoT-enabled SC. In the development and implementation of IS, risk is an unavoidable factor. Successful control of risk reduces an organization's operating risk. One of the key causes of IS failure is the weakness in risk management for IS growth, including prediction and evaluating risk [91,92]. IoT risk analysis requires the detection of assets, risks, and vulnerabilities. Failure to foresee and evaluate these vulnerabilities can lead to risks being generated. Other than that, the usage of poor application protection elements and the Application Programming Interface (API) can encourage a broad range of IS safety attacks [71,72]. In addition, the absence of a Smarter Security System to handle the identification of threats, the identification of anomalies, and the effects of predictive analysis affects IS performance [71]. Less secure and slower connections between IoT nodes lead to data leaks and other security breaches [74]. Another key element is availability and usability, which makes sure that the IS performs entirely at any time and every time an authenticated user is detected [17]. If any IS operation fails, the protection must ensure that equivalent resources are available, and as an added assurance, must allow M2M operations, i.e., real-time data collection will continue with IoT devices. Due to small and lightweight characteristics that make them operate on lower energy, the problems of resource constraint arises as most IoT devices have restricted handling and storage capacities [51]. Besides that, in medical practices, a network availability with effective admission to the patient's information is crucial, especially involving a system which contains important, sensitive, and potentially lifesaving information. Thus, the network must be available all the time [85].

The IoT technology enables users to be self-organized and personalized with data-driven decisions. Data-driven decision-making is a process that involves the collection of data based on established concrete objectives and the discovery of evidence, trends, associations, observations, and knowledge from this information. This expertise is then used to build or evaluate processes, operations, structures, policies, and techniques to support the data/system owner [5]. Information monitoring includes multi-device collaboration, which can effectively improve the accuracy and reliability of user-acquired information without fail. Another important problem is failure to collect the right data, as it can become a life-threatening matter for the citizens. Therefore, appropriate techniques can be used to ensure the IS is accurate, complete, reliable, and secure from malicious attacks during information transactions [52]. By using IoT technology, it allows information to be managed by machines, and enhances IS protection in the SC, such as protection against data leaks. By determining a corrective and preventive plan that

focuses on safety concern, each company in the SC needs to deliver a holistic risk management strategy.

## 5. Conclusion

This paper discusses the major challenges in the IS security management for IoT-enabled SCs. The document analysis discovers security challenges according to five aspects, namely: (i) governance, (ii) integrity, (iii) interoperability, (iv) personalization, and (v) self-organizing. It has been found that it is more complicated to protect IS from the heterogeneous IoT in SCs. At anytime, anywhere, and on any device, confidential data is exposed to malicious cyber-attacks. This study is expected to assist SC policy makers, city planners, and practitioners in understanding and addressing the challenges in sustaining IS security management for IoT-enabled SCs. This will lead to planning and the development of SCs to improve the citizens' quality of life. Future work must identify authentication features that are appropriate for IS security management by adopting IoT in SC environment. The aim is to overcome any unauthorized access to the sensitive and confidential information due to cyber-attacks.

## Conflict of Interest

The authors declare no conflict of interest.

## Acknowledgement

The study is supported by the Fundamental Research Grant Scheme (FRGS/1/2019/ICT04/UKM/03/2), 2019, Ministry of Education Malaysia and Universiti Kebangsaan Malaysia.

## References

[1] Z. Din, D.I. Jambari, M.M. Yusof, J. Yahaya, "Challenges in Managing Information Systems Security for Internet of Things-enabled Smart Cities," in 6th International Conference on Research and Innovation in Information Systems, IEEE, Bangi, Selangor Malaysia, 2019.

[2] United Nations, World Urbanization Prospects - The 2014 revision, United Nations, Department of Economic and Social Affairs, 2014.

[3] L. Pascu, The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018, Bitdefender, 1–18, 2018.

[4] R. Khatoun, S. Zeadally, "Smart Cities : Concepts, Architectures, Research Opportunities," Communications of The ACM, **59**(No. 8), 46–57, 2016.

[5] N. Mohamed, J. Al-Jaroodi, I. Jawhar, N. Kesserwan, "Data-Driven Security for Smart City Systems: Carving a Trail," IEEE Access, **8**, 147211–147230, 2020, doi:10.1109/access.2020.3015510.

[6] K.C. Laudon, J.P. Laudon, Management information systems : Managing The Digital Firm (15th Edition), Pearson Education Limited, London, 2018, doi:10.1007/978-94-017-9618-7_44.

[7] K. Sha, W. Wei, T.A. Yang, Z. Wang, W. Shi, "On security challenges and open issues in Internet of Things," Future Generation Computer Systems, **83**, 326–337, 2018, doi:10.1016/j.future.2018.01.059.

[8] J. Howell, Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says, IHS Markit, 2017.

[9] Y. Ye, T. Li, D. Adjeroh, S.S. Iyengar, "A Survey on Malware Detection Using Data Mining Techniques," ACM Computing Surveys, **50**(3), 41:1–41:40, 2017, doi:10.11648/j.ijiis.s.2014030601.16.

[10] H. Susanto, M.N. Almunawar, INFORMATION SECURITY MANAGEMENT SYSTEMS, Taylor & Francis Group, U.S, 2018.

[11] N. Yousefnezhad, A. Malhi, K. Främling, "Security in Product Lifecycle of IoT Devices : A Survey," in 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), Elsevier Ltd, San Francisco, CA,: 102779, 2015, doi:10.1016/j.jnca.2020.102779.

[12] M.P. Dijkers, "A beginner's guide to data stewardship and data sharing," Spinal Cord, **57**(3), 169–182, 2019, doi:10.1038/s41393-018-0232-6.

[13] N. Noori, T. Hoppe, M. de Jong, "Classifying pathways for smart city development: Comparing design, governance and implementation in Amsterdam, Barcelona, Dubai, and Abu Dhabi," Sustainability (Switzerland), **12**(10), 2020, doi:10.3390/SU12104030.

[14] N. Noori, M. De Jong, T. Hoppe, "smart cities Towards an Integrated Framework to Measure Smart City Readiness : The Case of Iranian Cities," Smart Cities, 676–704, 2020.

[15] A. Glaser, N. Jeambon, Smart City Platforms … and Aligning Technology and Citizens, 2018.

[16] A. Martinez-Balleste, P. Perez-Martinez, A. Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City is Possible," IEEE Communications Magazine, **51**(6), 136–141, 2013, doi:10.1109/MCOM.2013.6525606.

[17] A.E. Hassanien, M. Elhoseny, S.H. Ahmed, Amit Kumar Singh, Security in Smart Cities: Models, Applications, and Challenges, Springer Nature Switzerland AG 2019, Switzerland, 2019, doi:10.1007/978-3-030-01560-2.

[18] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, (February), 2011, doi:10.1109/WIRELESSVITAE.2011.5940923.

[19] L. Yang, N. Elisa, N. Eliot, Privacy and Security Aspects of E-Government in Smart Cities, Smart Cities Cybersecurity and Privacy, 89–102, 2018, doi:10.1016/b978-0-12-815032-0.00007-x.

[20] Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, M. Peacock, "Future challenges for smart cities: Cyber-security and digital forensics," Digital Investigation, **22**(August), 3–13, 2017, doi:10.1016/j.diin.2017.06.015.

[21] I. Nadir, Z. Ahmad, H. Mahmood, G. Asadullah Shah, F. Shahzad, M. Umair, H. Khan, U. Gulzar, "An auditing framework for vulnerability analysis of iot system," Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019, (October), 39–47, 2019, doi:10.1109/EuroSPW.2019.00011.

[22] M. Conti, A. Dehghantanha, K. Franke, S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, **78**, 544–546, 2018, doi:10.1016/j.future.2017.07.060.

[23] ISO/IEC, ISO/IEC 27001:2013, ISO, Switzerland, 2013.

[24] P.T.I. Lam, R. Ma, "Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study," Cities, **91**(August 2019), 146–156, 2018, doi:10.1016/j.cities.2018.11.014.

[25] K.C. Laudon, J.P. Laudon, A. Elragal, Management Information Systems: Managing the Digital Firm, 2016, doi:10.1590/S1415-65552003000100014.

[26] K. Salamzada, Z. Shukur, M.A.B.U. Bakar, "A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan," Asia-Pacific Journal of Information Technology and Multimedia, **4**(1), 1–10, 2015.

[27] Angraini, R.A. Alias, Okfalisa, "Information security policy compliance: Systematic literature review," Procedia Computer Science, **161**, 1216–1224, 2019, doi:10.1016/j.procs.2019.11.235.

[28] M.-D. Mclaughlin, J. Gogan, "Challenges and Best Practices in Information Security Management," Mis Quarterly Executive, **17**(3), 237–262, 2018.

[29] H. Paananen, M. Lapke, M. Siponen, "State of the art in information security policy development," Computers & Security, **88**, 101608, 2020, doi:10.1016/j.cose.2019.101608.

[30] M.A. Hasbini, T. Eldabi, A. Aldallal, "Investigating the information security management role in smart city organisations," World Journal of Entrepreneurship, Management and Sustainable Development, **14**(1), 86–98, 2018, doi:10.1108/WJEMSD-07-2017-0042.

[31] S. Al-janabi, I. Al-shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," Journal of Information & Knowledge Management, **15**(1), 1–30, 2016, doi:10.1142/S0219649216500076.

[32] R. Kitchin, "The real-time city ? Big data and smart urbanism," GeoJournal, **79**(November 2013), 1–14, 2014, doi:10.1007/s10708-013-9516-8.

[33] ITU, "Overview of the Internet of things," Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks, 1–22, 2012.

[34] M. Abomhara, Geir M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues," in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), IEEE, Aalborg, Denmark: 1–8, 2014, doi:10.1109/MC.2018.2888765.

[35] A.-R. Sadeghi, C. Wachsmann, M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE, San Francisco, CA, USA: 1–6, 2015, doi:10.1145/2744769.2747942.

[36] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, "Internet of

Things for Smart Cities," IEEE Internet of Things Journal, **1**(1), 22–32, 2014, doi:10.1109/JIOT.2014.2306328.
[37] M. Noor, W.H. Hassan, "Current research on Internet of Things ( IoT ) security : A survey," Computer Networks, **148**, 283–294, 2019, doi:10.1016/j.comnet.2018.11.025.
[38] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," Communications in Computer and Information Science, **89 CCIS**, 420–429, 2010, doi:10.1007/978-3-642-14478-3_42.
[39] C.E.A. Mulligan, M. Olsson, "Architectural implications of smart city business models: An evolutionary perspective," IEEE Communications Magazine, **51**(6), 80–85, 2013, doi:10.1109/MCOM.2013.6525599.
[40] H.F. Atlam, R.J. Walters, G.B. Wills, "Intelligence of Things : Opportunities & Challenges," in 3rd Cloudification of the Internet of Things (CIoT), IEEE: 1–6, 2018.
[41] M. Kanellos, Amount of Data Created Annually to Reach 180 Zettabytes in 2025, IDC, **2016**(March 7, 2016), 2016.
[42] R. Thirukkumaran, P. Muthu Kannan, "Survey: Security and Trust Management in Internet of Things," Proceedings - 2018 IEEE Global Conference on Wireless Computing and Networking, GCWCN 2018, 131–134, 2019, doi:10.1109/GCWCN.2018.8668640.
[43] L. O'Donnel, 2 Million IoT Devices Vulnerable to Complete Takeover, Threatpost.Com, 2019.
[44] A. Meola, What is the Internet of Things & How Does IoT Work, Business Insider, 2018.
[45] K.K. Patel, S.M. Patel, "Internet of Things-IOT : Definition , Characteristics , Architecture , Enabling Technologies , Application & Future Challenges," International Journal of Engineering Science and Computing, **6**(5), 6122–6131, 2016, doi:10.4010/2016.1482.
[46] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-porisini, "Security , privacy and trust in Internet of Things : The road ahead," Computer Networks, (January 2015), 2018, doi:10.1016/j.comnet.2014.11.008.
[47] L. Ismail, L. Zhang, Information Innovation Technology in Smart Cities, Springer Nature, 2018.
[48] H.F. Atlam, G.B. Wills, IoT Security, Privacy, Safety and Ethics, Springer Nature Switzerland AG 2020, Switzerland: 123–149, 2020, doi:10.1007/978-3-030-18732-3_8.
[49] A.S. Elmaghraby, M.M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," Journal of Advanced Research, **5**(4), 491–497, 2014, doi:10.1016/j.jare.2014.02.006.
[50] R.P. Dameri, Urban Smart Dashboard. Measuring Smart City Performance, 2017, doi:10.1007/978-3-319-45766-6.
[51] W. Aman, "Modeling Adaptive Security in IoT Driven e Health.pdf," in Norwegian Information Security Conference (2013), 61–69, 2013.
[52] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," Egyptian Informatics Journal, **18**(2), 113–122, 2017, doi:10.1016/j.eij.2016.11.001.
[53] J. Cho, A. Swami, I. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, **13**(4), 562–583, 2011.
[54] A. Merella, IoT security issues, risks and threats this year, Apiumhub, 2018.
[55] A. Aldairi, L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," Procedia Computer Science, **109**(2016), 1086–1091, 2017, doi:10.1016/j.procs.2017.05.391.
[56] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, **76**, 146–164, 2015, doi:10.1016/j.comnet.2014.11.008.
[57] R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, **57**(10), 2266–2279, 2013, doi:10.1016/j.comnet.2012.12.018.
[58] Z.K. Aldein Mohammeda, E.S. Ali Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies," World Scientific News, (February), 126–148, 2017.
[59] V. Mohammadi, A.M. Rahmani, A.M. Darwesh, A. Sahafi, "Trust - based recommendation systems in Internet of Things : a systematic literature review," Human-Centric Computing and Information Sciences, 1–61, 2019, doi:10.1186/s13673-019-0183-8.
[60] T.J. Ellis, Y. Levy, "A Systems Approach to Conduct an Effective Literature Review in Support of InformationThe Literature Review: The Foundation for Research," Informing Science Journal, **9**, 1–39, 2006.
[61] M. Ammar, G. Russello, B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, **38**, 8–27, 2018, doi:10.1016/j.jisa.2017.11.002.
[62] R.W.S. Ruhlandt, "The governance of smart cities: A systematic literature review," Cities The International Journal of Urban Policy and Planning, (October 2017), 1–23, 2018, doi:10.1016/j.cities.2018.02.014.
[63] N. Dong, J. Zhao, L. Yuan, Y. Kong, "Research on Information Security System of Smart City Based on Information Security Requirements," Journal of Physics: Conference Series, **1069**(1), 2018, doi:10.1088/1742-6596/1069/1/012040.
[64] A. Whitmore, A. Agarwal, L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, **17**(2), 261–274, 2015, doi:10.1007/s10796-014-9489-2.
[65] Y. Lu, L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, **6**(2), 2103–2115, 2019, doi:10.1109/JIOT.2018.2869847.
[66] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, P. Siano, "IoT-based smart cities: A survey," EEEIC 2016 - International Conference on Environment and Electrical Engineering, (June), 2016, doi:10.1109/EEEIC.2016.7555867.
[67] M.A. Wahab, D.I. Jambari, "Service Level Agreement Parameters for Drafting Public Sector Information System Contract," Jurnal Pengurusan, **52**, 153–167, 2018.
[68] R. Derakhshan, R. Turner, M. Mancini, "Project governance and stakeholders: a literature review," International Journal of Project Management, **37**(1), 98–116, 2019, doi:10.1016/j.ijproman.2018.10.007.
[69] M. Sookhak, H. Tang, Y. He, F.R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," IEEE Communications Surveys and Tutorials, **PP**(c), 1, 2018, doi:10.1109/COMST.2018.2867288.
[70] S. Ijaz, M. Ali, A. Khan, M. Ahmed, "Smart Cities: A Survey on Security Concerns," International Journal of Advanced Computer Science and Applications, **7**(2), 2016, doi:10.14569/ijacsa.2016.070277.
[71] M. Irshad, "A systematic review of information security frameworks in the internet of things (IoT)," Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016, 1270–1275, 2017, doi:10.1109/HPCC-SmartCity-DSS.2016.0180.
[72] Andrew van der Stock, B. Glas, N. Smithline, T. Gigler, OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, Creative Commons, **1**(1), 1–24, 2017, doi:10.1002/kin.550040606.
[73] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. (Sherman) Shen, Security and Privacy in Smart City Applications: Challenges and Solutions, 2017, doi:10.1080/00207168808803619.
[74] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, **20**(8), 2481–2501, 2014, doi:10.1007/s11276-014-0761-7.
[75] M.A. Hasbini, T. Eldabi, A. Aldallal, "Investigating the information security management role in smart city organisations," World Journal of Entrepreneurship, Management and Sustainable Development, **14**(1), 86–98, 2018, doi:10.1108/WJEMSD-07-2017-0042.
[76] Icon Labs, Floodgate Security Framework | Icon Labs, Icon Labs, 2019.
[77] J. Fan, P. Zhang, D.C. Yen, "G2G information sharing among government agencies," Information and Management, **51**(1), 120–128, 2014, doi:10.1016/j.im.2013.11.001.
[78] P. Radanliev, "Cyber Risk Management for the Internet of Things," University of Oxford, (April), 1–27, 2019, doi:10.13140/RG.2.2.34482.86722.
[79] A. Gharaibeh, M.A. Salahuddin, S.J. Hussini, A. Khreishah, I. Khalil, M. Guizani, A. Al-Fuqaha, "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," IEEE Communications Surveys and Tutorials, **19**(4), 2456–2501, 2017, doi:10.1109/COMST.2017.2736886.
[80] S. Theodorou, N. Sklavos, Chapter 3 - Blockchain-Based Security and Privacy in Smart Cities, Elsevier Inc., Greece: 21–37, 2019, doi:https://doi.org/10.1016/B978-0-12-815032-0.00003-2.
[81] V. Ekong, U. Ekong, "a Survey of Security Vulnerabilities in Wireless Sensor Networks," Nigerian Journal of Technology, **35**(2), 392, 2016, doi:10.4314/njt.v35i2.21.
[82] A.A.A. Al-Wosabi, Z. Shukur, "Proposed system architecture for integrity verification of embedded systems," Journal of Engineering and Applied Sciences, **12**(9), 2371–2376, 2017, doi:10.3923/jeasci.2017.2371.2376.
[83] A. Patel, S. Al-janabi, I. Alshourbaji, "A novel methodology towards a trusted environment in mashup web applications," Computers & Security, **49**, 107–122, 2014, doi:10.1016/j.cose.2014.10.009.
[84] P.P. Pereira, J. Eliasson, J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," IECON Proceedings (Industrial Electronics Conference), (November), 5293–5299, 2014, doi:10.1109/IECON.2014.7049308.
[85] G. Belleville, "Sit Down and Write Your Thesis! Practical and Motivational

Tips for Scientific Writing," Canadian Journal of Cardiology, **35**(8), 945–947, 2019, doi:10.1016/j.cjca.2019.04.011.

[86] D. Maheshwari, M. Janssen, "Reconceptualizing measuring, benchmarking for improving interoperability in smart ecosystems: The effect of ubiquitous data and crowdsourcing," Government Information Quarterly, **31**(SUPPL.1), 1–9, 2014, doi:10.1016/j.giq.2014.01.009.

[87] N.A. Azeez, T.M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, R. Ahuja, "Intrusion Detection and Prevention Systems: An Updated Review," Advances in Intelligent Systems and Computing, **1042**(January), 685–696, 2020, doi:10.1007/978-981-32-9949-8_48.

[88] H. Van Der Veer, A. Wiles, Achieving Technical Interoperability, France, 2008.

[89] S. Madakam, R. Ramaswamy, S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, **03**(05), 164–173, 2015, doi:10.4236/jcc.2015.35021.

[90] T.K. Sung, "Industry 4.0: A Korea perspective," Technological Forecasting and Social Change, **132**(November 2017), 40–45, 2018, doi:10.1016/j.techfore.2017.11.005.

[91] S.F. Abdullah, M.M. Yusof, D.I. Jambari, "Risk Management Model for Information Systems Planning in Public Sector," Jurnal Pengurusan, **48**, 149–160, 2016, doi:http://dx.doi.org/10.17576/pengurusan-2016-48-12 Model.

[92] B. Baharuddin, M.M. Yusof, "Evaluation of risk management practices in information systems project in the public sector," Jurnal Pengurusan, **53**, 20, 2018.