Information Systems Security Management for Internet of Things: Enabled Smart Cities Conceptual Framework

Zarina Din[a], Dian Indrayani Jambari[b], Maryati Mohd Yusof[c] and Jamaiah Yahaya[d]
Faculty of Information Science and Technology, National University of Malaysia, 43650, Bangi, Selangor, Malaysia

Keywords: Information Systems Security Management, Smart Cities, Internet of Things, Cybersecurity.

Abstract: Evolving Information Technology (IT) that drives the fourth Industrial Revolution (4IR) is disrupting organisational management. Particularly in public sector, the global movement towards Smart Cities (SC) initiative involving the Internet of Things (IoT) is motivating drastic changes to IT management methods. The heavy adoption of the IoT technologies in SC creates complexity for the information security to be managed by Information Systems (IS). IS security management approach changes according to the current nature of an organisation. As organisations prepare towards SC, there is a need to understand key concepts in managing IS security in IoT towards SC. The current IS security management for organisations is challenged in five aspects: governance, integrity, interoperability, personalisation, and self-organisation. Therefore, this study proposes an IS security conceptual framework for IoT management towards realising SC. Literature review uses the document analysis method to identify key concepts on relevant reports, for the purpose of developing a proposed conceptual framework. Based on analysis from previous research, a conceptual framework for IS Security Management in IoT-enabled SC was proposed as the outcome of this study.

1 INTRODUCTION

Smart cities utilise information and communication technologies to enhance the quality of life for citizens, local authority activities, and communication within government. Technology is ubiquitous, so smart cities use information and communication technologies to make life easier for citizens by circumventing traffic congestions for users, informing users in real-time about available services, or notifying users regarding any urban transformation (Harrison et al. 2010). With the Internet at every place, urban infrastructure which consists of various types of electronics or smart devices, such as surveillance cameras, notifies citizens about traffic conditions, assesses air pollution using sensors, and uses smart tools to manage domestic consumption of electricity, gas, etc. Cities are becoming more and more intelligent with the expansion of digital technology (connected objects, 4G / 5G mobile networks, etc.) (Witti & Konstantas 2019). Following the relevance of smart cities to numerous stakeholders, and the advantages and challenges pertaining to its implementation, the concept of smart cities has drawn essential attention from researchers within multiple fields, including IoT, IS, and more areas of computer science and engineering disciplines (Ismagilova et al., 2019).

2 BACKGROUND

SC is a citizen-centric urban operation that is sustainable and innovative via the use of IT to improve the present and future citizens' quality of life, sustainability, continuous urbanisation, and intelligence. The concept of "smart city" implies the development of an urban ecosystem, in which the government, businesses, and citizens actively use digital technologies to collect and analyse

[a] https://orcid.org/0000-0003-0987-8066
[b] https://orcid.org/0000-0001-6700-1815
[c] https://orcid.org/0000-0003-4286-2939
[d] https://orcid.org/0000-0003-2429-4114

Din, Z., Jambari, D., Yusof, M. and Yahaya, J.
Information Systems Security Management for Internet of Things: Enabled Smart Cities Conceptual Framework.
DOI: 10.5220/0009791700440051
In *Proceedings of the 9th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2020)*, pages 44-51
ISBN: 978-989-758-418-3

information and exchange data to create and maintain the effective life of a "smart person" in time and space. Yigitcanlar and Kamruzzaman (2018) defines that a city becomes "smart" when it starts to use digital technologies actively in all areas of its economic activities. The public's accessibility in utilising such technologies increases the demand for service providers in both public and private sectors to provide high quality service.

IoT is an enabler for cultivating smarter society through its application in vital public service domains, such as healthcare, transportation, agriculture, energy, and security. Gartner reported that the number of IoT devices entering households will drastically increase from nine devices per household to 500 devices by 2022, with IoT connectivity being bundled into products (Nathan Nuttall, 2018). This revelation, together with the prediction that 70% of global population will be living in cities by 2050, is driving the conceptualisation of IoT-enabled SC. In addition, Gartner's Survey Analysis 2016 on Internet of Things Backbone showed that security is a top barrier to IoT success, followed by the complexity of implementation and integration, privacy concern, potential risks and liabilities, and the technology itself being immature (Ganguli & Friedman, 2017). Organisations need to be able to keep abreast with IoT technologies which will impact their IoT initiatives, attempt IoT technology to ensure the success of IoT projects, and overcome these difficulties.

City platforms which are based on IoT and other smart devices must be protected from attackers or unauthorised access. Due to the use of the Internet, IoT receives the same vulnerabilities as any other computing device, possibly becoming a cyber-attack victim. An attack on a connected device can cause substantial damage on a SC platform and impact serious vulnerability issues. Besides, confidential information may also be accessed from any connected device over the network (Witti & Konstantas, 2019). To ensure a successful SC development, security must be highlighted and improved. Thus, the public sector is required to improve their organisational management, services, systems functionality, information sharing and integration, and business process coordination. This shows that it is integral to reform the IS management in public sector organisations, despite challenges.

However, assessment on readiness of the IS performance in IoT-enabled SC indicates that the existing IS management approach for managing IS security in SC operation is deemed to be unsuitable or unfit (Lam & Ma, 2018). IS security management is problematic in several ways: (i) IS is unprepared to manage ongoing threats of cyber-attacks, as it is vulnerable to information leaks and access breaches (Wahab & Jambari, 2018); (ii) IS is poorly designed for IoT-enabled SC, as security measures are not properly defined (Mah, 2015); and (iii) the application of IoT threatens the IS interoperability, particularly concerning the incompatibility of IoT technology with legacy IS that remains critical to operation (Lam & Ma, 2018; Laudon & Laudon, 2018). The complex security concerns indicate the diverse perspectives for IS security in IoT-enabled SC. Existing studies have focused on investigating IS security and providing security solutions from a technical perspective, while research on the management perspective is limited (Whitmore, Agarwal & Da Xu, 2015). Lam and Ma (2018) suggested that IS security management should be addressed through governance by establishing appropriate and clear IS security management standards, and proper cyber-attack and remedial plan strategies. Control measures for IS operation's planning and management are also crucial to improve security management (Abdullah, Yusof & Jambari, 2016).

The aim of this study is to develop a conceptual framework for IS security management for IoT-enabled SC based on the five (5) components: (i) governance; (ii) integrity; (iii) interoperability; (iv) personalisation; and (v) self-organisation, to achieve secure and high-quality IS. The framework is developed through document analysis on relevant published articles and reports. The conceptual framework serves as the foundation for a comprehensive and practical solution to support a more effective IS security management for SC. This paper is organised as follows: It starts with research introduction and proceeds with the research background. The next section focuses on literature review. The fourth section explains the research methodology used in this study. Subsequently, the remaining sections will describe the result and discussion of the proposed conceptual framework for IS security management for IoT-enabled SC. The last section addresses concluding remarks by highlighting the research contribution, together with suggestions for future research work.

3 LITERATURE REVIEW

This part of the paper discusses the literature on the management of IS security for IoT-enabled SC, which is important for considering IS security management and IoT Security management simultaneously. All SC stakeholders will get valuable and secure information in IoT ecosystems, which is security issues become a major concern. Reliable, economical and efficient security including privacy for IoT is needed to ensure the appropriate confidentiality, integrity, authentication and access control among others.

3.1 IS Security Management in SC

The SC initiative will integrate IS and emerging IT, such as IoT, into urban development to enable government functionality, city operations, services deliveries, and intelligent analytics that will enhance public services, production, and usability. These are essential backbones for connecting the core IS together in a city. As information creation and sources become dynamic, the IS is exposed to different security attacks and critical vulnerabilities (Kumar et al., 2018). IS security in IoT-enabled SC involves issues in technology, applications, infrastructure, and information, which are affected by the emergent integration of IoT, leading to intensive communication, high complexity, and high interdependency. Cyber security, particularly in IS for IoT-enabled SC, is challenged by the difficulty to ensure end-to-end security via large and interdependent IS, with multiple stakeholders involved, and incompatible data standards and formats for integration. The IS security concerns specifically with IoT applications in SC, including attacks on data confidentiality, threats to data integrity (Dunkerley & Tejay, 2009; Gil-Garcia, Pardo & Nam, 2015; Witti & Konstantas, 2019), misuse of resources, bandwidth degradation, battery or resources exhaustion, unauthorised access (Gharaibeh et al., 2017; Hassanien et al., 2019; Zedadra et al., 2019), threats to authentication, and Denial of Service (DoS).

Furthermore, the characteristics of SC require higher speed communication, more constant engagement between multiple organisations, and appropriate governance agenda (Ruhlandt, 2018) such as policy (Bull & Azennoud, 2016; Irshad, 2017; Lam & Ma, 2018; Laudon & Laudon, 2018; Ruhlandt, 2018; Theodorou & Sklavos, 2019; Trček, 2003; Whitmore et al., 2015; Witti & Konstantas, 2019), accountability (Hassanien et al., 2019; Irshad, 2017; Ruhlandt, 2018; Witti & Konstantas, 2019), and auditability (Hassanien et al., 2019; Irshad, 2017; Laudon & Laudon, 2018; Ruhlandt, 2018; Witti & Konstantas, 2019). Information integrity and systems security have always been vital in IS management. However, the various information types from multiple technologies and processing platforms in SC have also heightened the criticality in ensuring information integrity and systems security (Gichoya, 2005). Fast and reliable technology (Gharaibeh et al., 2017; Harrison et al., 2010; Taewoo Nam & Theresa A. Pardo, 2011; Witti & Konstantas, 2019) and communication between multiple organisations to integrate information, also affect the IS interoperability, as integration becomes more complex.

3.2 IoT Security Management in SC

The security aspects, such as communication confidentiality (Gharaibeh et al., 2017; Hassanien et al., 2019; Witti & Konstantas, 2019; Zedadra et al., 2019), authenticity (Gharaibeh et al., 2017; Hassanien et al., 2019; Witti & Konstantas, 2019; Zedadra et al., 2019), trustworthiness of communication partners (Aldein Mohammeda & Ali Ahmed, 2017; Hassanien et al., 2019), message integrity, and other requirements need to be highlighted in IoT. The challenges in the application of IoT-enabled SC are to the citizens' security and privacy, whenever their personal and private information is collected and analysed in IoT platform. It will be exposed to vulnerabilities and several attacks, so it is important to manage the way citizens and service providers are able to control the information and how they are exposed to third-party applications (Moreno et al., 2017). There is a necessity to access certain services or prevent from communicating with other things in IoT (Aldein Mohammeda & Ali Ahmed, 2017).

Furthermore, IS in IoT-enabled SC is connected to the IoT application context. Authorities as service providers, must analyse their target, specify the required computing hardware and software, and finally, integrate these heterogeneous subsystems. The existence of such infrastructure and the provision of an appropriate collaborating structure among IS can be a huge challenging task for the IoT-based IS (Arasteh et al., 2016). Such complexity in the communication among IS in IoT environment is problematic to the interoperability of the IS, due to non-standard heterogeneous interfaces in IS (Lam & Ma, 2018). Additionally, each type of smart object in IoT has different information, processing, and communication capabilities; and subjected to different conditions, such as energy availability and the communications bandwidth required. To facilitate communication and cooperation of these objects, common standards are required (Aldein Mohammeda & Ali Ahmed, 2017). The reliability problem has become significant in IoT-based systems due to numerous smart devices involved (Arasteh et al., 2016).

Thus, IoT security management should consider two (2) dimensions: personalisation and self-organisation. The personalisation feature requires access to the citizens' private and personal information from multiple IS that manage the information gathered and processed via IoT devices (Arasteh et al., 2016; Dong et al., 2018; Elmaghraby & Losavio, 2014; Ferraz & Ferraz, 2014; Hassanien et al., 2019; Irshad, 2017; Lam & Ma, 2018; Laudon & Laudon, 2018; Nagamalla & Varanasi, 2017; Trček, 2003; Whitmore et al., 2015; Witti & Konstantas, 2019). This issue challenges IS security in IoT-enabled SC. As massive citizens' connected devices generate staggering volume of information instantaneously (Gharaibeh et al., 2017), the risks of cyber-attacks such as Distributed Destruction of Service (DDoS) attacks on public infrastructure potentially increase. Such risks highlight the difficulty to manage secured information exchange during the communication and integration of multiple IS to enable citizen-centric services (Aldairi & Tawalbeh, 2017).

Meanwhile, the Self-organisation feature would allow direct machine-to-machine (M2M) communication over the internet through IoT devices (Whitmore et al., 2015). Self-organisation is the management of accepting, processing, and distributing information using automated M2M without human involvement (Aldein Mohammeda & Ali Ahmed, 2017; Lam & Ma, 2018; Sung, 2018). Machines are operated independently or coordinate with humans to produce customer-oriented manufacturing that constantly works to maintain itself and be made available at every time (Aldein Mohammeda & Ali Ahmed, 2017; Hassanien et al., 2019; Lam & Ma, 2018; Mohanty, Choppali & Kougianos, 2016; Sung, 2018; Witti & Konstantas, 2019). Hence, the machines become independent entities that can collect and analyse data, and provide advice based on the analysis (Sung, 2018), which will cause risk on IS integrity. Risk is one important aspect in managing IS security in IoT-enabled SC (Dong et al., 2018; Gharaibeh et al., 2017; Harrison et al., 2010; Irshad, 2017; Nagamalla & Varanasi, 2017). Less effective risk management in IS will become one of the causes of failure of IS security management in organisations (Abdullah et al., 2016; Baharuddin & Yusof, 2018). Risk analysis in IoT consists of identifying assets, threats, and vulnerabilities. Another important factor is availability, which is to ensure that IS performs completely at any time, every time it detects an authenticated user (Hassanien et al., 2019). The security must ensure that corresponding resources are available if any IS operation fails, and as an added assurance, must allow M2M operations. The use of IoT technology that enables machines to manage information will boost IS security in the SC, such as against information leaks.

To propose a conceptual framework for IS security management for IoT-enabled SC, this study will consider both aspects of security management: IS security management in SC, and IoT security management in SC. Therefore, this conceptual framework will be categorised into five (5) dimensions: governance, integrity, interoperability, personalization, and self-organisation.

4 METHODOLOGY

Qualitative method has been adopted for this study. Document analysis was performed by gathering, and critically analysing documented reports on related topics to the scope of the study. It was conducted to identify the key concepts of IS and IoT security management in SC. The documents include scientific articles, research theses, and government official documents. The Scientific articles were gathered from several databases related to the computing field such as Scopus, Web of Science, IEEE, Science Direct, Springer Link, and ACM Digital Library. Besides that, research reports in the form of theses and books were also gathered for data collection and analysis. Related government official documents were also gathered from publicly available sources, including government official portals and document libraries. The searching process used Open search engines, such as Google, Google scholar, and research gates. The keywords used were "information system security management," "smart cities," "Internet of Things" and "cybersecurity" from 2014 to 2019. Only journals, conference proceedings, books, and working papers written in English and Malay were selected for this study. Document analysis method was then applied to analyse the reports according to the defined keywords. The analysis resulted in the identification of five key concepts and established their relationship with IS security management in IoT towards SC development.

5 RESULT AND DISCUSSION

The establishment of SC requires IS security management for IoT to address issues of unauthorised access of sensitive and confidential information due to cyber-attacks. Besides that, reliability, integrity, availability, and real-time information to the citizen (Giffinger et al., 2007) were also highlighted. The proposed conceptual framework was developed based on the five (5) dimensions for managing IS security for IoT in SC, consisting of governance, integrity, interoperability, personalisation, and self-organisation. Each dimension has a relationship, as illustrated in Figure 1.

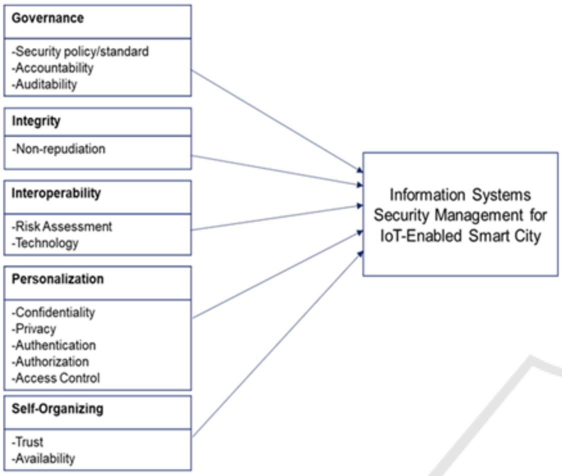

Figure 1: Proposed Conceptual Framework for Information System Security Management for Internet of Things (IoT)-enable Smart Cities.

The description of each dimensions in the proposed conceptual framework are as follows:

5.1 Governance

Governance is identified as the anchoring concept for improving the IS security management for IoT in SC. Governance needs to be redefined according to the features of SC for IS integrity, interoperability, personalisation, and self-organisation. Governance contains strategies, policies, and frameworks as a guide for organisations in ensuring effective IS management to support organisational strategies and objectives (Laudon & Laudon, 2018). Besides that, the different range of IS security levels from various SC organizations integrated will be overcome. Three (3) elements are related to this study: security policy/standard, accountability, and auditability.

i. Security policy/standard: IS security standard/policy refers to the document that contains specification of information security and standardisation of requirement to ensure information quality in SC, by using IoT technology. Compliance to the policy and standard is very important to ensure interoperability and to prevent from taking risks. (Lam & Ma, 2018; Laudon & Laudon 2018; Theodorou & Sklavos, 2019; Trček, 2003; Whitmore et al., 2015; Witti & Konstantas, 2019)

ii. Accountability: Accountability refers to the person or device, who has generated and processed the information. Accountability assurance can assist in the heterogenous IoT environment to specify which device has generated which data and which device has processed which data (Hassanien et al., 2019; Nia & Jha, 2016). It is an ability to ensure that users are held responsible for their actions.

iii. Auditability: refer to the ability of a system to perform continuous and consistent monitoring of all actions (Hassanien et al., 2019; Nia & Jha, 2016) such as collecting, processing, and transmitting an information.

5.2 Integrity

Managing the IS Integrity is crucial for SC to ensure quality information for accurate decision making. Integrity has four (4) characteristics, i.e. completeness, timeliness, accuracy, and validity of the information managed by IS (Dunkerley & Tejay, 2009; Flowerday & Von Solms, 2005). It will prevent unauthorised users from manipulating even a single bit of data in the communication, ensuring completeness and accuracy (Hassanien et al., 2019; Nia & Jha, 2016). In the IoT, integrity concerns become critical when it comes to the modification of information in daily life activities such as medical records, financial transactions, etc. The non-repudiation element was identified to influence integrity dimension.

i. Non-repudiation: Non-repudiation is defined as a system’s confirmation action whether an event has happened or not. The policy must strictly be enforced regarding event occurrence (Hassanien et al., 2019; Nia & Jha, 2016).

5.3 Interoperability

Another affected IS security management is interoperability. Interoperability is defined as the ability of IS to support the business processes for data exchange, and information and knowledge sharing (Gharaibeh et al., 2017). An organisation must have the ability to communicate and transfer data effectively by using different information systems in terms of infrastructure, geographical area, and culture (Van Der Veer & Wiles, 2008). The organisations' readiness to use IoT is still low and requires an integrated link among various devices, services, and applications due to the use of different technologies offered by IS suppliers. This study proposed risk assessment and technology to be elements that influence IS security management for IoT in SC.

i. Risk Assessment: This refers to identifying, estimating, and prioritising risks to SC operations, organisational assets, individuals, and other organisations, resulting from the use of IoT in IS. The risk analysis of IoT is by identifying the assets, threats, and vulnerabilities (Dong et al., 2018; Irshad, 2017; Nagamalla & Varanasi, 2017).

ii. Technology: Technology involves using a series of information security technology to realise security protection of the physical environment, network transmission, host system, data resources, and applications services in SC (Harrison et al., 2010; Taewoo Nam & Theresa A. Pardo, 2011).

5.4 Personalisation

The services are provided uniquely and specifically, depending on the profile and individual needs (Gharaibeh et al., 2017). As result, the privacy of citizens' personal data will become vulnerable to the threat. For this study, researcher will use confidentiality, privacy, authentication, authorisation, and access control to represent personalisation elements.

i. Confidentiality: Confidentiality refers to the act of ensuring that only authorised users access the information and that the information must be confidentially transmitted from sensor devices to storage (Hassanien et al., 2019; Nia & Jha, 2016). In the IoT, devices collect various sensitive information from the users, so identity and details of information can be tracked by unknown users.

ii. Privacy: Privacy can be defined as 'not even a single bit of information of a person will be revealed to anyone else without the consent of the owner.' In the IoT, most sensors which are part of public services will collect numerous personal information, but to whom personal information can/should be shared, must be decided by the individual owner (Hassanien et al., 2019).

iii. Authentication: Authentication (i.e. to confirm identification) means communicating parties interact using the authenticated counterparts. Successful authentication mechanism ensures confidentiality, integrity, and availability of information. Authentication in the IoT becomes critical due to the heterogeneity of the number of devices involved (Liu, Xiao & Chen, 2012). Each device transmits data or wants access to other devices; therefore, each user is required to authenticate oneself to gain access from sensors.

iv. Authorisation: Authorisation is related to the users' or IoT devices' permission to access sensitive information in SC environment. The authentication process will permit authorised users to access the data (Witti & Konstantas, 2019).

v. Access Control: This signifies that only authenticated users or devices can access other individuals' data and devices (Liu et al., 2012). IS Security management must ensure the accuracy of information by preventing the modification of information by unauthorised users.

5.5 Self-organisation

IoT technology facilitates the reception, processing, and distribution of personal information without human intervention. Information system communication is automated via machine-to-machine (M2M) without having to wait for human instructions (Aldein Mohammeda & Ali Ahmed, 2017; Lam & Ma, 2018; Sung, 2018). Besides increase in productivity, there is also vulnerable for hacking. Connecting to more devices means more vulnerabilities. This study proposed two (2) elements that influence IS security management for IoT in SC in the self-organisation dimension.

i. Trust: Trust can be defined as ensuring that the people and devices involved in IoT system accept the services and information with full faith and confidentiality (Nia & Jha, 2016). Trust management involves reliable data collection, reliable data combination and mining, and enhanced user privacy. IS must be reliable on real-time data (Shwe, Jet & Chong, 2016). Successful trust in IS security will ensure quality of IoT services.

ii. Availability: This refers to the assurance that all services are available and operated in the complete system at any time without fail, when requested by an authenticated user (Hassanien et al., 2019; Nia & Jha, 2016). Availability in the security can be guaranteed by the sufficient resources, whenever required.

6 CONCLUSIONS

A conceptual framework for IS security management in IoT-enabled SC is important to establish the understanding of the key concepts in managing IS security in IoT towards the development of SC. Extensive literature review has verified the proposed conceptual framework. This study has categorised five (5) general dimensions in IS Security Management for IoT-enabled SC, comprising governance, integrity, interoperability, personalisation, and self-organisation. Most IoT devices or information may be exposed to information security threats and vulnerabilities if not correctly secured and will become a challenge to develop secure IoT ecosystems. In addition, the verification of the conceptual framework by selected experts had been done completely. Future work is already planned for developing a comprehensive framework and validation based on empirical work. The result achieved will become a guide for SC authorities to enhance their IS security management in IoT-enabled SC.

ACKNOWLEDGEMENTS

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

REFERENCES

Abdullah, S. F., Yusof, M. M. & Jambari, D. I. 2016. Risk Management Model for Information Systems Planning in Public Sector. *Jurnal Pengurusan*, *48*, 149–160.

Aldairi, A. & Tawalbeh, L. 2017. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109*(2016), 1086–1091.

Aldein Mohammeda, Z. K. & Ali Ahmed, E. S. 2017. Internet of Things Applications, Challenges and Related Future Technologies. *World Scientific News*, (February), 126–148. Retrieved from www.worldscientificnews.com

Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-khah, M. & Siano, P. 2016. IoT-based smart cities: A survey. *EEEIC 2016 - International Conference on Environment and Electrical Engineering*, (June).

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

Bull, R. & Azennoud, M. 2016. Smart citizens for smart cities: participating in the future. *Proceedings of the Institution of Civil Engineers - Energy*, *169*(3), 93–101.

Dong, N., Zhao, J., Yuan, L. & Kong, Y. 2018. Research on Information Security System of Smart City Based on Information Security Requirements. *Journal of Physics: Conference Series*, *1069*(1).

Dunkerley, K. & Tejay, G. 2009. Developing an Information Systems Security Success Model for eGovernment Context. *Americas Conference on Information Systems (AMCIS) 2009 Proceedings. 346.*, 59–60.

Elmaghraby, A. S. & Losavio, M. M. 2014. Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497.

Ferraz, F. S. & Ferraz, C. A. G. 2014. *Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment. Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014*,.

Flowerday, S. & Von Solms, R. 2005. Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers and Security*, *24*(8), 604–613.

Ganguli, S. & Friedman, T. 2017. *IoT Technology Disruptions : A Gartner Trend Insight Report. Gartner*,. Stamford USA. Retrieved from https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/3738060-iot-technology-disruptions-a-gartner-trend-insight-report.pdf

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M. & Al-Fuqaha, A. 2017. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Communications Surveys and Tutorials*, *19*(4), 2456–2501.

Gichoya, D. 2005. Factors Affecting the Successful Implementation of ICT Project in Government. *The electronic Journal of E Government*, *3*(4), 175–184.

Giffinger, R., Fertner, C., Kramar, H. & Meijers, E. 2007. City-ranking of European Medium-Sized Cities. http://www.smartcity-ranking.eu/download/city_ranking_final.pdf [15 January 2019].

Gil-Garcia, J. R., Pardo, T. A. & Nam, T. 2015. What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization. *Information Polity*, *20*(1), 61–87.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. & Williams, P. 2010. Foundations for Smarter Cities. *IBM Journal of Research and Development*, *54*(4), 1–16.

Hassanien, A. E., Elhoseny, M., Ahmed, S. H. & Amit Kumar Singh. 2019. *Security in Smart Cities: Models, Applications, and Challenges*.

Irshad, M. 2017. 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.

Ismagilova, E., Hughes, L., Dwivedi, Y. K. & Raman, K. R. 2019. Smart cities: Advances in research—An information systems perspective. *International Journal of Information Management*, *47*(January), 88–100.

Kumar, H., Singh, M. K., Gupta, M. P. & Madaan, J. 2018. Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. *Technological Forecasting and Social Change*, (October 2017), 1–16.

Lam, P. T. I. & Ma, R. 2018. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities*, *91*(August 2019), 146–156.

Laudon, K. C. & Laudon, J. P. 2018. *Management information systems : Managing The Digital Firm (15th Edition)*. *New York*, hlm.Vol. Fifteenth. London: Pearson Education Limited.

Liu, J., Xiao, Y. & Chen, C. L. P. 2012. Internet of things ' authentication and access control. *Int. J. Security and Networks*, *7*(4), 18–21.

Mah, P. 2015. Lessons from the Singapore Exchange failure. *Singapore Exchange Board Committee of Inquiry*,.

Mohanty, S. P., Choppali, U. & Kougianos, E. 2016. Everything You Wanted to Know About Smart Cities. *IEEE Consumer Electronics Magazine, 5(3), 60–70.*, (July), 1–15.

Moreno, M. V., Terroso-Saenz, F., Gonzalez-Vidal, A., Valdes-Vela, M., Skarmeta, A. F., Zamora, M. A. & Chang, V. 2017. Applicability of Big Data Techniques to Smart Cities Deployments. *IEEE Transactions on Industrial Informatics*, *13*(2), 800–809.

Nagamalla, V. & Varanasi, A. 2017. A review of security frameworks for Internet of Things. *2017 International Conference on Information Communication and Embedded Systems, ICICES 2017*, (Icices).

Nathan Nuttall. 2018. *The Evolution of IoT and Its Impact on Adopters and Technology Providers: A Gartner Trend Insight Report*. Stamford USA.

Nia, A. M. & Jha, N. K. 2016. A Comprehensive Study of Security of IoT. *IEEE Transactions on Emerging Topics in Computing*, *6750*(c), 1–19.

Ruhlandt, R. W. S. 2018. The governance of smart cities: A systematic literature review. *Cities The International Journal of Urban Policy and Planning*, (October 2017), 1–23.

Shwe, H. Y., Jet, T. K. & Chong, P. H. J. 2016. An IoT-oriented data storage framework in smart city applications. *2016 International Conference on Information and Communication Technology Convergence, ICTC 2016*, 106–108.

Sung, T. K. 2018. Industry 4.0: A Korea perspective. *Technological Forecasting and Social Change*, *132*(November 2017), 40–45.

Taewoo Nam & Theresa A. Pardo. 2011. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. *The Proceedings of the 12th Annual International Conference on Digital Government Research services*, *12th Annua*, 282–291.

Theodorou, S. & Sklavos, N. 2019. Chapter 3 - Blockchain-Based Security and Privacy in Smart Cities. *Smart Cities Cybersecurity and Privacy*, hlm.21–37. Greece: Elsevier Inc.

Trček, D. 2003. An Integral Framework for Information Systems Security Management. *Computers & Security*, *22*(4), 337–360.

Van Der Veer, H. & Wiles, A. 2008. *Achieving Technical Interoperability*. *European Telecommunications Standards Institute*, 3rd Edition. France.

Wahab, M. A. & Jambari, D. I. 2018. Service Level Agreement Parameters for Drafting Public Sector Information System Contract. *Jurnal Pengurusan*, *52*, 153–167.

Whitmore, A., Agarwal, A. & Da Xu, L. 2015. The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.

Witti, M. & Konstantas, D. 2019. A Secure and Privacy-preserving Internet of Things Framework for Smart City. *ICIT*, 145–150.

Yigitcanlar, T. & Kamruzzaman, M. 2018. Does smart city policy lead to sustainability of cities? *Land Use Policy*, *73*(November 2017), 49–58.

Zedadra, O., Guerrieri, A., Jouandeau, N., Seridi, H. & Fortino, G. 2019. Swarm Intelligence and IoT-Based Smart Cities: A Review. *The Internet of Things for Smart Urban Ecosystems*, hlm.1–24. Springer International Publishing.