https://doi.org/10.48009/3_iis_2020_227-235

Issues in Information Systems
Volume 21, Issue 3, pp. 227-235, 2020

INTERNET OF THINGS (IOT) MEDICAL SECURITY: TAXONOMY AND PERCEPTION

Anne Shepherd, Robert Morris University, vasst262@mail.rmu.edu
Chalermpon Kesa, Robert Morris University, cxkst116@mail.rmu.edu
James Cooper, Robert Morris University, jecst232@mail.rmu.edu

ABSTRACT

With technology advances, IoT applications are proliferating in the medical field. Integration of endpoint devices, sensors, communications, and applications is leading to improved data availability and tools to manage positive healthcare outcomes. However, in healthcare failures and security leaks can damage or be lethal to patients and jeopardize trust in providers and health care organizations. This study empirically develops an IoT Medical taxonomy with implications for categorizing and matching IoT security in the healthcare field to users by: (1) identifying the characteristics of IoT security and (2) describing and testing users' perceptions. The research analyzes the users' perceptions of IoT Medical security in terms of the fundamental issues such as confidentiality, integrity, availability, authentication, authorization, and audit. In addition to the proposed taxonomy of IoT Medical security, we summarize the key security factors influencing the users making the decision to use IoT. The study will help improve IoT security architecture design, IoT product development, and inform decision-making on IoT medical technology.

Keywords: Taxonomy, IoT, IoT medical, Security, Perceptions, confidentiality, integrity, availability, authentication, authorization, and audit

The Internet and cyberspace integration of the digital and physical world has become a reality and continues to transform our lives. This paradigm shift, referred to as the 4th industrial revolution, has implications for our life experiences from jobs to healthcare. Internet of Things (IoT) is a major element in the next industrial revolution (Wellener et al, 2019). Experts predicted the Internet of Things, (IoTs) to expand to more than 35 billion devices connecting to existing networks and infrastructures in 2020 (Maayan, 2020). The ability to connect devices that have uniquely addressable Internet Protocol (IP) spaces created the concept of the Internet of Things. IoT devices provide the sensoring and controlling of objects across an existing network or corporate infrastructure. The direct integration between physical objects such as vehicles, refrigerators, smart phones, and medical devices are examples of IoT devices. New protocols facilitate the connection between people, objects and computer systems.

Some of the driving forces for the IoTs are low cost of hardware, sensors, and microprocessors. The low cost of hardware in the past years on both the computer and supporting components coupled with low manufacturing cost of the devices. Additionally, communication via wireless connection and new intelligent protocol management platforms is a forcing function. Wireless connections are ready and available at restaurants, hospitals, airports, and other public spaces. The advancement in communication protocols allow these direct connections with little effort on the part of the end users (Video Internet of Things Overview, 2020).

Security concerns stem from the rapid pace of the technology evolution which leaves security considerations behind for the convenience of connections and exchanging data with these networks. Traditional networks An IoT device connected to medical devices, paired with a network could lead to an attack on the individual using a medical IoT device. One of the characteristics of IoT devices that create a greater impact from cyber-attack is design to be unobtrusive in nature often embedded in systems without user intervention and transparent to users (Video Internet of Things Overview, 2020). Traditional networks are described as a collection of different types of devices managed and administratively configured by skilled personnel within an organization, (Oppenheimer, 2011). A self-healing network is de-centralized in nature and not managed or configured by skilled professional. These networks detect potential problems and mitigate them with minimal human intervention. The independent ability of self-healing networks to detect and mitigate issues create a heterogeneous network (Dala, 2014). This heterogeneous design leaves out the mitigation that could cause the attack (Video Internet of Things Overview, 2020).

LITERATURE REVIEW

Connected technology such as the Internet of Things (IoT) has become embedded in our daily lives. In the healthcare industry, for example, we are doing things we have never done before. In response to the global pandemic in 2020, IoT devices and sensors are used to track patient temperature data for predictive analytics and potential virus outbreak geographic areas (i.e. hotspots). With digital transformation comes the expectation and requirement for secure technology innovation. Security is foundational to advanced technology such as IoT.

Internet of Things (IoT) is the next era in the IT world and emerging from its infancy and transforming it into an integrated part of Internet (Matharu et al., 2014). However, research pertaining to IOT security is nascent, therefore, our research addresses the imperative to understand the risks, threats and vulnerabilities to ascertain the possible security approaches needed to fully integrate and apply to the IoT (Gaur et al., 2015).

IoT Security

Risk management is the process of identifying risk, assessing risk, and reducing risk to an acceptable level in which we understand and respond to the factors that may lead to a failure in the confidentiality, integrity, or availability of an information system (Gary, Alice & Alexis, 2002). Information security risk is the harm to a process or accidental events (SANS Institute, 2020).

Dorsemaine, Gaulier, Wary and Kheir (2015) proposed a taxonomy for the Internet of Things (IoT). Dorsemaine et al describe IoT as “infrastructures interconnecting connected objects”, focusing on the local endpoints as specific to IoT. The authors IOT taxonomy categorizes IOT into five object groups: energy, communication, functional, local users and hardware/software resources that can apply to various vertical markets including healthcare. For both communication and hardware/software objects security is an important attribute in the IoT taxonomy.

There are four factors information integrity, confidentiality, accountability, and availability that serve as critical information security objectives (Johnston & Michael, 2008). Mendez et al, 2017, mention the necessity of communication protocol in order to find a feasible solution for system protection at the application level which includes IEEE 802.15.4 Security, Zigbee and Tiny OS protocols. Some security requirements established in order to consider IoT nodes as secure are data confidentiality, integrity, freshness, availability, organization autonomy, and authentication. Figure 1 depicts a general IoT architecture. Regardless of the architecture components, the Sans Institute IoT survey concluded that security is a challenge for IoT and will increase vulnerabilities in a big way (Pescatore & Shpantzer, 2014)). Further the study purported the IoT security conundrum presents an opportunity for “new ways of thinking about the ecologies of security” (Pescatore & Shpantzer, 2014), p 10).

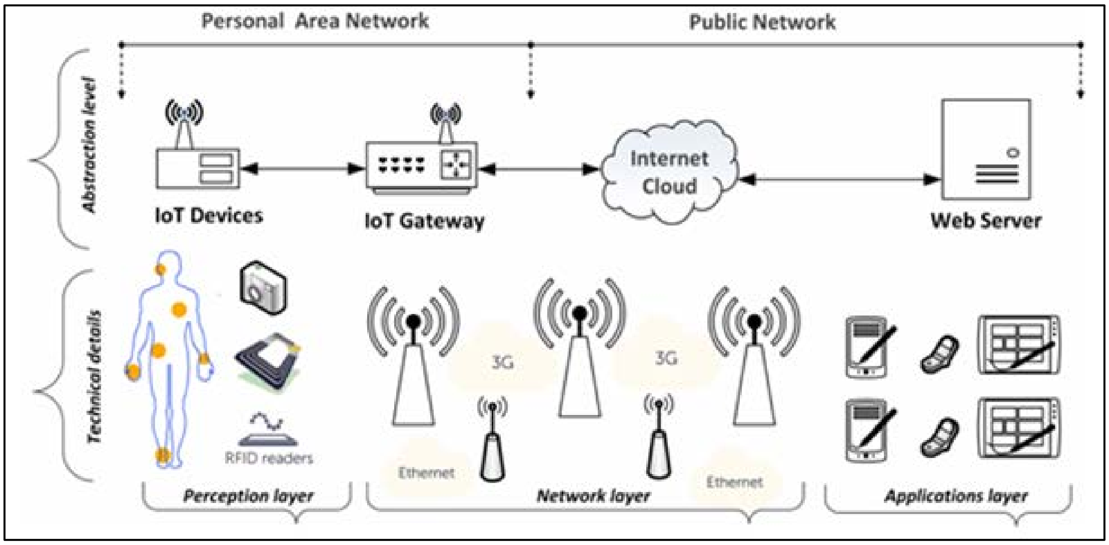

Figure 1. A Generic Architecture of an IoT system.

From the generic architecture above, IoT can be classified into three layers (Zhao and Ge, 2013), namely, application, perception, and network protocol as shown in the Figure 2. The application layer which is visible to the end-user can be structured in several ways based on the service it offers (Jing et al., 2014). The security issues differ depending on the industry. The perception layer involves the collection of information, which is classified into two sections, namely, the perception node (sensors, controllers, and so on) and the perception network that interconnects the network layer (Jing et al., 2014). The network layer provides network transmission and information security and delivers pervasive access environment to the perception layer. The network layer includes mobile devices, cloud computing, and the Internet (Pongle and Chavan, 2015).

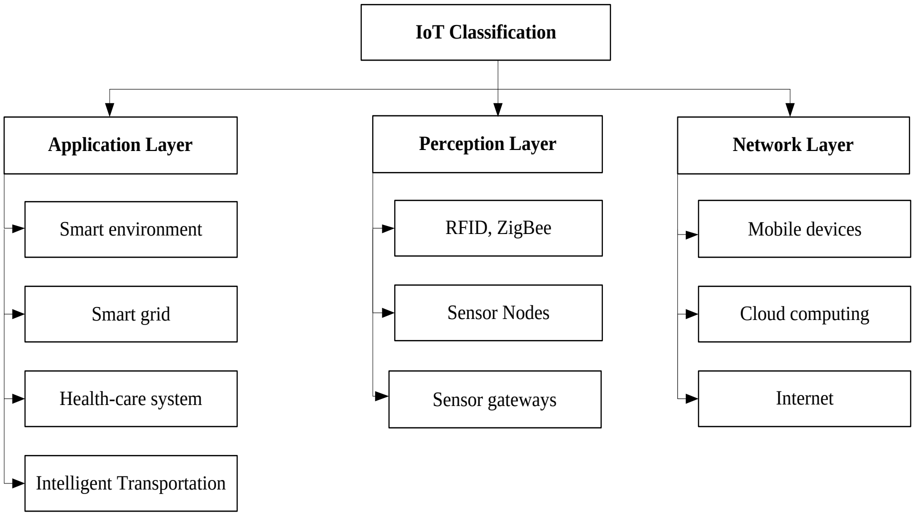

Figure 2. IoT Classification (Zhao & Ge, 2013)

In Figure 3, the IoT security Taxonomy addresses the IoT architecture and important factors from an IoT security perspective (Alaba et al, 2017). The taxonomy addresses several of the faults and shortcomings of previous works and present current security threats in the contexts of application, architecture, communication and data (Alaba et al, 2017). The most commonly used security techniques that are considered with the use cases in this application domain are (i) authentication, (ii) authorization, (iii) exhaustion of resources, and (iv) trust establishment.

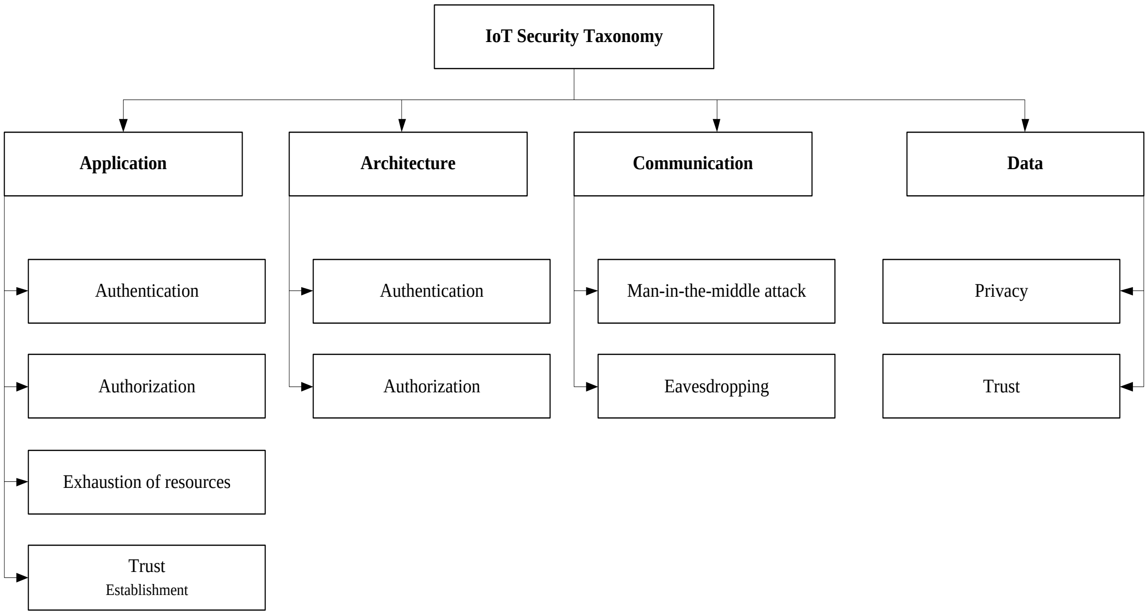

Figure 3. IoT Security Taxonomy

The various security frameworks and taxonomies indicate the complexities and different approaches for securing IoT devices and platforms. Our research aims to understand security in the healthcare domain. Later in this research we propose an IoT Security Taxonomy for the medical domain. Limited security research has focused on IoT for the healthcare sector and extended to the end user.

Threats in IoT Medical

The STRIDE threat model, a cybersecurity guiding principle, addresses a wide range of security threats holistically. This model can be an effective tool in the arsenal to mitigate infrastructure threats and counter unknown threats associated with IoT medical devices (Adam Shostack, 2008 p.61-63).

The STRIDE threat model attributes are 1) Spoofing which is the pretending to be something or someone other than yourself. The security property violated is authentication. 2) Tampering is modifying something on disk, on a network or memory. The security property tampering violates integrity. 3) Repudiation is claiming that a user did not do something or was not responsible for the action committed. The security property violated is non-repudiation. 4) Information Disclosure is providing information to someone not authorized to see it. The security property violated is confidentiality. 5) Denial of Service is absorbing resources needed to provide service. The property violated is Availability. 6) Elevation of Privilege is allowing someone to do something they are not authorized to do.

Security threats for a healthcare application can present catastrophic outcomes. From a healthcare IoT perspective data security implies data is stored and transferred securely to assure integrity, validity, an authenticity (Sun et al, 2018). Additionally, for mobile devices used in healthcare the attacks aim to confiscate and control user data, control device resources and control applications.

IoT devices, supported by open technology and platforms, are inherently prone to security vulnerabilities. IoT devices should evolve to more “self-dependence” in identifying and correcting security invasions (Solongi et al, 2018).

Ray, Jones & Zhang (2013) discuss identity theft, software control and connectivity as safety threats for patients. Their study elaborates on threats in the home healthcare environment in comparison to hospitals and other healthcare organizations.

Vulnerabilities in IoT Medical

As in most domains, IoT in healthcare can be susceptible to security vulnerabilities. In healthcare IoT every physical object is locatable and therefore vulnerable. "Vulnerabilities of IoT reside in devices, communication, service applications and by exploiting vulnerabilities attacks are launched" (Ge & Kim, 2015, p 776). Medical device security is perplexing as suppliers and medical organizations attempt to balance performance, usability and safety vulnerabilities.

An IoT sensor, the multi-hub relay system that connects the source nodes, as well as other network applications require measures against common attacks which include Denial of Service (DoS), traffic analysis, node replication (Sybil attack), general confidentiality concerns, black hole routing attacks and physical damage or unauthorized manipulation (Mendez, Papapanagiotou & Yang, 2017).

Wireless devices prevalent in healthcare applications magnify exposure to data leaks and malware. Mobile device and Bluetooth protocols like 802.1x and Zigbee are vulnerable to data being intercepted. IoT security issues arise pertaining to data integrity because mobile devices are potential targets for malicious attacks (Tarouco et al, 2012, p.6123).

Taxonomy of IoT Medical Security

The proposed taxonomy of IoT medical security as shown in the figure 4, is based on the previous studies and security best practices as a systematic approach. This classification focuses on the factors: security, user, threat, data, IoT technology, and communication as a holistic view of IoT medical security. It will facilitate security professionals understanding users' perceptions and the important factors of IoT medical security, and improve IoT medical security architecture, IoT product development and enhance decision making of IoT medical in term a security.

The IoT medical taxonomy considers people, process, and technology. It is for patients and healthcare organizations to understand and assess the importance of security factors in decisions.

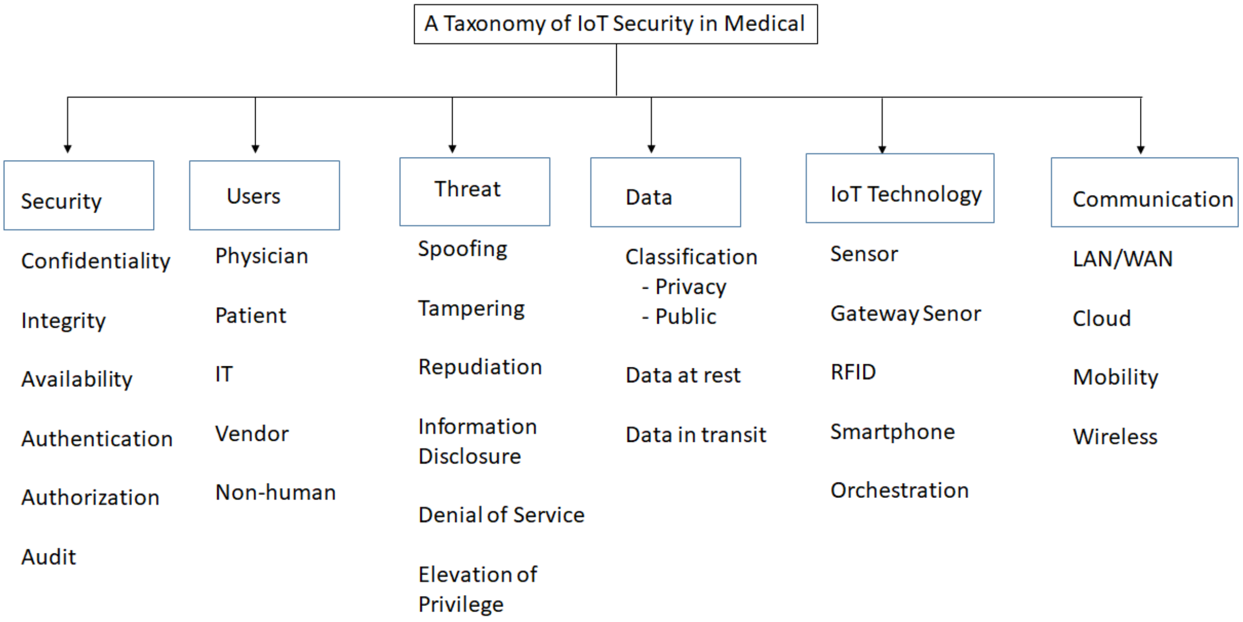

Figure 4. Proposed IoT Medical Security Taxonomy

Security

HIPPA and other health care policies require extensive security measures in the medical area. Confidentiality is important to ensure data is secure and only available to authorized users. Integrity ensures that data is being received from the right sender and to ensure that the data is not tampered with during transmission due to intended or unintended interference. Availability is focused on the data being present when it is needed. Each IoT medical object must be clearly identifiable and authenticated. Healthcare applications rely on authorization of access rights to resources such as medical devices and are dependent on trust. Finally, auditing requires routinely reviewing audit logs for compliance with security principles and processes (Alaba et al, 2017, Johnston & Pearson, 2008).

Users

The human related problems are on all levels of the organization, from uninformed end-users such as a patient, physician, IT professional, vendor, administrative staff to upper management. Although technical security controls such as firewalls, anti-virus, and auditing are easy to be implemented, they are not sufficient to ensure the achievement of multiple information security objectives (Johnston & Pearson, 2008). In IoT the term user includes human as well as machines and services, and it also includes the internal objects (i.e. devices that are part of the network) and external objects. Therefore, security should include users and tools which contribute to improved IoT security decisions.

Threat

As discussed earlier in this research the STRIDE threat model is foundational to IoT security. The STRIDE threat model has been used in the design of secure software systems [8] and applied to security threats to RFID. (Thompson, Sunkara & Thompson, 2006). RFID technology is frequently used in the design of IoT medical applications. IoT medical threat characteristics in the proposed taxonomy include: 1) Spoofing Identity such as to replace an authorized reader with an unauthorized reader and reads the tags of an individual without the individual's authorization 2) Tampering with data 3) Repudiation such as actions against tracking RFID tags 4) Information Disclosure 5) Denial of Service by deletion or modification of the serial number in an RFID-enabled device and Elevation of Privileges to grant unauthorized access.

Data

Data from this view is the inputs and outputs of the medical IoT architectural components and processes. In healthcare IoT context patient data is in a static state or in motion. Data at rest is stored in the IoT device, on the network or in a workflow process. Alternatively, data in transit is flowing over a secured or unsecured network. For example, end user devices such as an iPad or blood pressure monitoring device can store data at rest internal to the IoT device.

IoT Technology

The medical IoT technology stack comprises sensors, gateways, RFID tags, smartphones and an orchestration layer. The sensors and objects collect data; gateways act as interface points to IoT platforms; RFID radio frequency tags attach to objects and send data; intelligent phones facilitate communication and orchestration provides a single unified view into data across the technology platform.

Communication

Healthcare IoT leverages communication for network access control and data flow from the endpoint to the healthcare provider or organization. For security and resilience diverse communication technology may be used in healthcare IoT solutions. Healthcare IoT communication at the network layer includes LAN/WAN access and transport, wireless connectivity, cloud technology and mobility.

RESEARCH QUESTION

To accomplish the goal of this study, the research addresses the following research questions:

RQ1: What are the users' perceptions of IoT Medical technology risk in terms of security, threat, and vulnerability?

RQ2: What is the ranking of the key security factors to support decision making when selecting Medical IoT technology?

METHODOLOGY

Survey research has the advantage of explaining outcomes in terms of other effects, and participant responses are considered statistical evidence (Check & Schutt, 2012). To conduct the study, the quantitative approach is used in the form of a survey instrument. Data collection methods and a questionnaire approach are used to find the users' perceptions of IoT Medical technology risk in terms of security, threat, and vulnerability, and the important security factors for decision making when selecting Medical IoT technology. The Likert-type scale is used to measure the perception of users on IoT Medical security. Using scale: 1= Strongly Disagree, 2= Disagree, 3= Neutral, 4= Agree, 5= Strongly Agree.

Data Collection. This study chose the purposive sample as fundamental to the quality of data gathered (Bernard, 2002). According to Bernard (2002) in a study of cloud computing adoption in enterprises (Carcary, Doherty, & Conway, 2013) used 1500 SMEs and "aimed for a response rate of 7% in order to achieve 100 usable responses, which were deemed a suitable minimal level in a large population" (Harrigan, Rosenthal, & Scherer, 2008).

The study conducts a sample size of 170 participants related to IoT Medical such as patients, physicians, IT professionals, administrators, and vendors. A pilot test is used to refine the test instrument and specific issues addressed including question ambiguity, the refinement of the research protocol, and the confirmation of scale reliability (Van and Hundley, 2001).

Data Analysis. The overall statistical finding of demographic data. The research questions, survey questionnaire, and analysis tools are the sources for the data analysis strategy for this study.

CONCLUSION

The main contribution of this paper is a medical security taxonomy. This taxonomy calls for further research as is proposed as a next step with the survey questions and data analysis. Our survey will assess the completeness of the survey itself as an instrument for IoT medical. Another expected result is the importance and prioritization of factors pertaining to IoT medical security.

REFERENCES

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28

Ali, B., & Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors 2018, 18, 817.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010, July). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications* (pp. 420-429). Springer, Berlin, Heidelberg.

Bernard, H.R. (2002). Research Methods in Anthropology: Qualitative and quantitative methods. 3rd edition. AltaMira Press, Walnut Creek, California.

Carcary, M., Doherty, E., & Conway, G. (2013). The adoption of cloud computing by Irish SMEs: An exploratory study. The Electronic Journal Information Systems Evaluation, 16(1), 258–269.

Check J., & Schutt R. K. (2012). Survey research. Research methods in education. Thousand Oaks, CA. Sage Publications; 2012. pp. 159–185.

Dalal A.C., "A framework for self-healing home networks," *10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, Rhodes, 2014, pp. 135-136, doi: 10.1109/QSHINE.2014.6928674

Dorsemaine, B., Gaulier, J. P., Wary, J. P., Kheir, N., & Urien, P. (2015, September). Internet of things: a definition & taxonomy. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 72-77). IEEE.

Gary, S., Alice, G., & Alexis, F. (2002). Risk Management Guide for Information Technology Systems. NIST National Institute of Standards and Technology, NIST Special Publication 800-30.

Gaur, A., Scotney, B., Parr, G., and McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science*, *52*(1), 1089–1094.

Ge, M., & Kim, D. S. (2015, December). A framework for modeling and assessing security of the internet of things. In *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 776-781). IEEE.

Harrigan, J.A., Rosenthal, R., & Scherer, K. (2008). New handbook of methods in non-verbal behaviour research. Oxford: Oxford University Press.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). "Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ser. ASIA CCS '16. New York, NY, USA: ACM, pp. 461–472.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481–2501.

Johnston, Q., A. & Pearson, J. (2008), "Information security management objectives and practices: a parsimonious framework", Information Management & Computer Security, Vol. 16 No. 3, pp. 251-70.

Lu, C. (2014). Overview of Security and Privacy Issues in the Internet of Things, 1–11.

Matharu, G.S., Upadhyay, P., & Chaudhary, L. (2014). The Internet of Things: Challenges & security issues. in Emerging Technologies (ICET), International Conference on, IEEE.

Maayan, G. D. (2020). The IoT Rundown For 2020: Stats, Risks, and Solutions. *Security Today*, https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?p=1

Mendez, D.M., Papapanagiotou, I., Yang, B. (2017). Internet of things: Survey on security and privacy. Eprint arXiv:1707.01879.

Paul Wellener et al, *2019 Deloitte and MAPI Smart Factory Study: Capturing value through the digital journey*, Deloitte Insights and MAPI.

Pescatore, J., & Shpantzer, G. (2014). Securing the internet of things survey. *SANS Institute*, 1-22.

SANS Institute. (2020). An Introduction to information system risk management http://www.sans.org/reading_room/whitepapers/auditing/an_introduction _to_information _system_risk_management_1204?show= 1204.php &cat= auditing

Solangi, Z. A., Solangi, Y. A., Chandio, S., bin Hamzah, M. S., & Shah, A. (2018, May). The future of data privacy and security concerns in Internet of Things. In *2018 IEEE International Conference on Innovative Research and Development (ICIRD)* (pp. 1-4). IEEE.

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. *Security and Communication Networks*, *2018*.

Ray, A., Jones, P., & Zhang, Y. (2013). Medical device security-a new frontier. *Biomedical instrumentation & technology*, *47*(1), 72.

Tarouco, L. M. R., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M. R., Carbone, F., Marotta, M., & De Santanna, J. J. C. (2012, June). Internet of Things in healthcare: Interoperatibility and security issues. In *2012 IEEE international conference on communications (ICC)* (pp. 6121-6125). IEEE.

Thompson, D. R., Chaudhry, N., & Thompson, C. W. (2006). “RFID security threat model,” in Proc. Acxiom Laboratory for Applied Research (ALAR) Conf. on Applied Research in Information Technology.

Van Teijlingen ER., & Hundley, V. (2001). The Importance of Pilot Studies. Social Research Update. Retrieved from http://sru.soc.surrey.ac.uk/SRU35.html

Video Internet of Things Overview (Skillsoft), (2020). *Internet of Things overview* [Streaming Video]. Retrieved from MITRE Institute

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet Things Journal.

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 663–667.