Pre-Print: 2nd IEEE International Conference on Electrical, Control and Instrumentation engineering (ICECIE 2020), will be available in IEEE Xplore

A Framework to Address Security Concerns in Three Layers of IoT

Alwyn Jose[1], Sami Azam[1], Asif Karim[1], Bharanidharan Shanmugam[1*], Fahad Faisal[2], Ashraful Islam[3], Friso De Boer[1], Mirjam Jonkman[1]

[1] College of Engineering, IT and Environment, Charles Darwin University, NT, Australia
[2] Department of Computer Science and Engineering, Daffodil International University, Bangladesh
[3] School of Computing and Informatics, University of Louisiana at Lafayette, USA

Corresponding author: bharanidharan.shanmugam@cdu.edu.au

***Abstract*— The Internet of Things (IoT) is becoming part of many aspects of our life, including healthcare, home utilities, retail, energy, logistics, etc. This prolific and ubiquitous nature of IoT based systems brings with it the threats of cyber-attacks in a variety of forms. An IoT framework is a set of controlling rules, standards and protocols which makes implementation of IoT applications somewhat streamlined. However, due to the existence of a plethora of IoT devices, applications and technologies, standardization of IoT protocols is a complex undertaking. Several well-known IT organizations have their own customized standards for the IoT platform. However, the lack of stable standardization has been a prime concern for quite some time. This research outlines the overall technologies used in IoT security implementation and an overview of different threats faced by IoT devices. The work also recommends a security framework that can effectively be implemented with various IoT based systems.**

Keywords—IoT, privacy, security, cryptography, Internet of Things.

I. INTRODUCTION

The Internet of Things (IoT) has become an indispensable aspect of our daily lives. Almost all sectors have been benefited from its usefulness: industrial applications, homes, automobiles, health industry, entertainment and many more. The deployment of IoT creates new avenues for improvements in many of our regular day to day activities. This not only creates opportunities to unleash hidden benefits and comforts, but also introduces new job opportunities for various related sectors. The advantages of IoT are not limited to the personal sphere, but also to industry and the global economy as a whole.

However, with such abundance of possibilities, there also arise issues of security and privacy. IoT devices these days generate a large amount of data, in the range of terabytes. Whether IoT can effectively safeguard the user's privacy or not is still debatable. IoT can be summarized as the interconnection of 'smart things' over the internet where 'things' communicate with each other for a purpose with an expected outcome depending on conditions [1, 11]. With the growing number of IoT devices, the need to identify security flaws in IoT has become one of the top priorities. The solution may lie in the standardization.

II. PERCEPTION ON IOT SECURITY AND CONCERNS

Figure 1 illustrates the outcome of a survey conducted by SANS Institute [2] on IoT security. It is estimated from the above figure that about 48.8 percent (A) of the people felt that IoT will have the same threats faced as the current Internet applications, while about 17.2 % people think that IoT will be a security disaster. Figure 2 shows another survey result from SANS [2] and results are also summarised in Table 1.

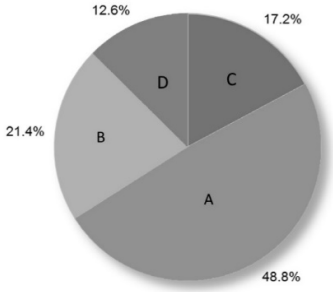

Fig. 1. Survey on IoT security

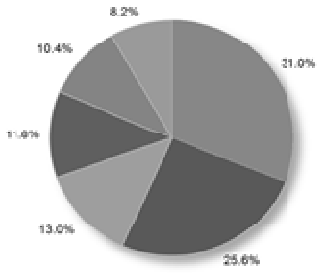

Fig. 2. A survey on IoT threats [2]

A. Major Security Concern

There are several security protocol standards such as WEP 802.11 IEEE, IPSec and SSL (Secure Socket Layer) to implement security for transferring data and several cryptographic algorithms to address security challenges related to authentication, data integrity, user privacy and authorization. The limited computational capabilities of embedded systems, however, often limits the capacity of these security measures even though the protocols used may be the same. Figure 3 contains a summary of the main

978-1-7281-9877-4/20/$31.00 ©2020 IEEE

Table 1: Summary of IoT threat survey

Percentage (Decreasing Order)	Threats or Attack Vectors
31 %	Leaving things vulnerable due to no updates or update methods for patching vulnerabilities
25.6 %	Vulnerable devices can compromise an entire enterprise
13 %	DoS attacks to cause service interruptions, resulting in infrastructure damages or even loss of life
11.8 %	Intentional attacks on IoT devices to sabotage or for destruction
10.4 %	Damages caused by user error

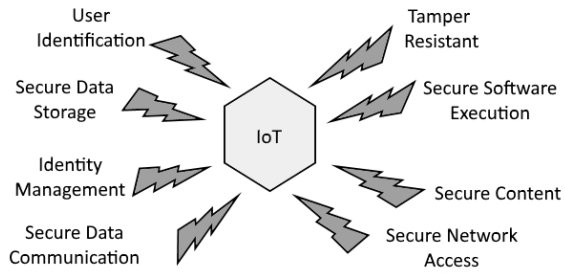

Fig. 3. Major security concern for IoT [4]

security aspects of IoT embedded devices. The major security concerns shown in figure 9 are dissected below [4]:

- **User Identification:** Process of authenticating a user before providing access to the system [27].
- **Secure Data Storage:** Involves mandatory security requirement of data integrity and confidentiality of data stored in the system.
- **Identity Management:** Process of managing users or devices in a system, by giving appropriate access or restrictions to resources.
- **Secure Data Communication:** This involves authentication of nodes, validating the authenticity of the received data, preventing rejection of a valid communication transaction and protecting the identities of entities involved.
- **Tamper Resistant:** This refers to the property of a device to maintain the integrity, even if it falls in the hands of an attacker, after being physically probed.
- **Secure Execution:** This involves the running of a firmware or software in a secure environment, to avoid execution of codes deviating from usual accepted standard.
- **Secure Content:** Digital Rights Management (DRM) secures the rights of the digital materials in the system.
- **Secure Network Access:** Ensures that a device can only be connected to a network after proper authorization.
- Besides, the importance of using TLS/DTLS (Transport Layer Security/Datagram Transport Layer Security) protocol in confirming end-to-end security has also been highlighted in recent research works [5].

Secure Data Storage: Involves mandatory security requirements of data integrity and confidentiality of data stored in the system.

B. Challenges in Establishing a Secure IoT

A number of papers address the major challenges in operational and technical features with the existing Internet security protocols [6-8]. Mixing the internet protocols with highly resource constrained networks will result in complex design of protocols and challenges in the overall operation of the system due to the heterogeneity of the networks involved [6]. Some of the common bottlenecks are:

- Resource Constraints: IoT uses very low bandwidth channels for communicating between different devices. The use of low-bandwidth by IoT devices is intentional due to the low memory, CPU and power supply constraints. The use of this low resource embedded device itself provides a vector for attack, as for example the IEEE 802.15.4 (LR-WPANs) are only able to send a frame of up to 127 bytes. This will result in the splitting of large packets of security protocols, giving rise to attack vectors for Denial of Service attacks. Sending several packets could lead to downgrading the overall system performance, especially if the fragmented packets are lost [8].
- Resistance to Denial of Service: The low memory, CPU and power supply constraints in IoT can invite resource exhaustion attacks to the unattended M2M (Machine-to-Machine) communications. These attacks are hard to find, and can only be found after the service is interrupted. DTLS (Datagram Transport Layer Security), IKEv2 (Internet Key Exchange version 2), HIP (Host Identity Protocol) and Diet HIP are the existing countermeasures for DoS attacks. However, the success of these techniques entirely depends on the routing capabilities of the network. It has also been argued that puzzle-based mechanisms are most viable solution in protecting IoT devices against DoS attacks as HIP works by sending cryptographic puzzles to the initiator of a connection for solving, the difficulties of these puzzles are variable, this could force an initiator off the connection. But, IoT devices with its weak computational power will not be able to solve the puzzle, which would consequently end the connection to the initiator [8].

C. IoT Privacy Requirements

Privacy can be strengthened by firstly understanding the need of IoT technologies and enhancing the technologies related to privacy issues and secondly by regulating the operations of IoT and thereby creating a legal framework to protect privacy and flow of data [9].

According to a survey conducted by Trend Micro Inc. in 2016, 44 percent of the people were concerned about their privacy [6]. Only the demand of consumers for secure IoT devices can change the attitude of major IoT device vendors to come up with a secure configuration [10]. There are a

number of IoT privacy and security such as: protecting the location of the person from the device associated, protecting very sensitive personal information through monitoring the Internet of Things devices used, localizing the data as much as possible by using a decentralized authentication key management, and by limiting the amount of unnecessary data that is needed to identify the user [15].

The following security and privacy requirements have been identified [12, 15]:

- **Resilience to Attacks:** The device should not fail after an attack over the network. It should fine-tune itself after any device failure and restart services.
- **Data Security:** All data entering and exiting the network should have appropriate authentication.
- **Data Access Control:** The flow of data could be controlled by the information providers. An efficient method has been discussed in [13].
- **User Privacy:** Only the provider should have access to user data, and this only under strict guidelines for providing services.

D. Security Threats and Privacy Requirements for SOA based IoT Middleware

Iinformation these days is often processed within a vast array of computing devices, connected through networks [14]. Previous studies have shed light on how the middleware system has grown from simply hiding network protocols to handling more complex tasks such as communication between two network devices to handling data and managing security. Furthermore, there have been multiple challenges faced by the service-oriented architecture (SOA). Security is one of the major challenges which demands a security architecture standard based on a service oriented architecture to safeguard the data [15-16].

An attack on IoT middleware can be of three types; Entities Attack, Data Attack and Communication Channel Attack. Entities Attack happens when there is unauthorized access and physical tampering of the device itself. Data Attacks occur when there is a manipulation in data or the presence of man in the middle such as eavesdropping during data exchange [16]. An attack on two system entities' communication is a Communication Channel Attacks [16].

E. Security Threats and Requirements for Cloud based IoT

Threats on cloud based IoT are real because of the lack of privacy preserving authentication mechanisms. There are six major threats [17], which are:

- Layer attack
- Identity privacy
- Location privacy
- Attack on the node
- Malicious cloud security
- Forward and backward attack

III. TYPES OF ATTACKS ON IOT DEVICES

Attacks on IoT embedded devices are rapidly rising [4], Table 2 shows some of the major attacks.

Denial of Services attacks have been particularly widespread. Such attacks seem to cause interruption through the misuse of available resources. Interruptions can be observed through packet loss, delays in communication and an overall degradation of the service provided. Consequences can quickly get worse as described earlier. To stop this situation, several techniques have been proposed such as Hash Chains (based on Cryptographic Hash algorithms) and Message Authentication Codes [18], Content Chaining using Hash Chains [19], Distributed Firewall [20] etc.

A. Security Threats in Different IoT application domain

Result of a survey on four key domain applications: Smart Environment [29], Smart Grid, Smart Health Care Systems and Smart Transport have been summarized in Table 3 [21].

After an extensive literature review, it has been understood that, threats and attacks can be targeted towards any devices in any IoT domains based on the environment. The attack vectors might also depend on the IoT device in use and its network connection type as shown in Figure 4.

IV. A PROPOSED FRAMEWORK

IoT consists of three main layers: Application, Network and Perception and every layer has its own related security concerns. In this section, a framework to address security concerns will be presented, that can be integrated into Application, Network and Perception Layer. The effectiveness and suitability of the proposed framework will also be evaluated. One of the major issues regarding implementing security sub-systems in IoT is that IoT devices cannot completely rely on network or transport layer encryption [22]. This is due to their constrained resources.

Application Layer: Security in the application layer is one of the crucial issues in an IoT framework due to its major role due to the features it provides such as UDP (User Datagram Protocol) or TCP (Transmission Control Protocol), the type of architecture, security, and quality of service, header size and so forth [23]. The interconnections between applications is made possible in the IoT by the application layer protocols. Some of the application layer protocols are CoAP (Constrained Application Protocol), MQTT (Message Queue Telemetry Transport), AMQP (Advance Message Queuing Protocol) and XMPP (Extensible Messaging and Presence Protocol) [24].

To select an appropriate protocol, which can be universally used by all IoT devices, standardization of

Table 2: Summary of attacks on IoT based systems [4]

	a) Physical Attacks	• Chip de-packaging • Micro-probing • Particle Beam Techniques
	b) Side Channel Attacks	• Timing Attacks • Power Analysis • Environmental Attacks • Electromagnetic Attacks

Attacks on IoT Device [3]		• Fault Analysis
	c) Cryptanalysis Attacks	• Cipher-text-only Attack • Known-plain text Attack • Chosen-plain text Attack • Man in the Middle Attacks
	d) Software Attacks	• Buffer Overflow • Virus • Trojan Horse • Logic Bombs • Denial of Service
	e) Network Attack	***Passive Attacks*** • Monitor and Eavesdropping • Traffic Analysis • Camouflage ***Active Attacks*** • Denial of Service Attacks • Node Subversion • Node Malfunction • Node Capture • Node Outage • Message Corruption • False Node • Replication Attacks • Routing Attacks

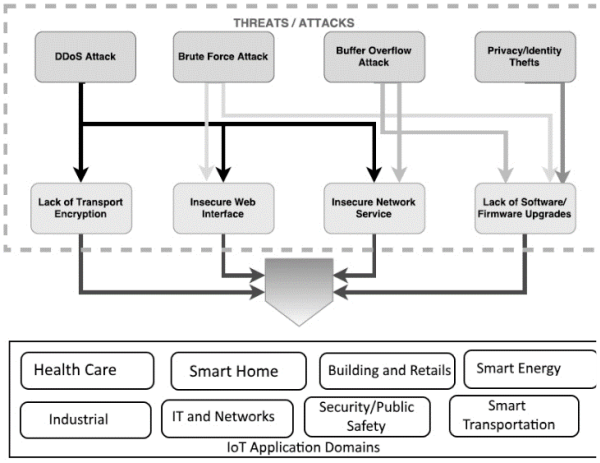

Fig.4 Any IoT based domains can be under threats and attacks [26]

IoT is required. However, to evaluate the best protocol that can be used in the application layer, a comparison study of its features can aid in this process. Table 6 shows comparison between some of the major protocols

Table 3: Application domain survey summary [21]

Application	***Network Communi-cation***	***Threats***	***Attacks***
Smart Environment	ZigBee, Bluetooth, LTE, LTE-A, Wifi, Ultra-wide band	Privacy, Eavesdropping, Authentication, Authorization,	Mobile Apps, Sensors
Smart Grid	ZigBee, Z wave, Wifi	Privacy, Eavesdropping, Physical attack, Device Tampering	End points on devices, Malici-ous Attacks
Smart Health	ZigBee, Bluetooth	Privacy, Authentication, Authorization, Denial of Service	Internal Attack, Cyber Attack
Smart Transportation	DSRC 8.5 GHz	Jamming, Congestion, Security and Spectrum Sharing	Cyber Attacks

From the comparison Table 6, the most suitable protocol which can be selected for constrained devices are CoAP and MQTT. Both protocols have very low CPU and memory usage compared to other protocols, and are therefore appropriate for constrained devices. However, the basis on which the IoT works is its ability to provide real time data. Due to the high sampling rate and latency of MQTT, this protocol cannot be used for real time applications. The Constrained Application Protocol (CoAP) is selected as the best protocol for the application layer. The selection of a protocol in an application layer depends on the fact whether CoAP over DTLS can be used instead of UDP, which enables ECC (Elliptic Curve Cryptography) support for RawPublicKey and Certificates.

Perception Layer: The perception layer is a physical layer consisting of sensors, such as location sensors, proximity sensors, magnetometers and sensors for measuring pressure, humidity, light density etc. The Perception layer also includes RFID (Radio Frequency Identification) tags, Zigbee, Bluetooth etc, as the main communication method used in transmission of data collected is through a wireless network [26, 28]. These wireless networks cannot be limited within strict boundaries and are therefore publically available. Anyone can monitor, intercept or disrupt these signals if proper security measures are not in place. This can directly affect the integrity of the data collected by the sensors or the nodes. Data collected in the perception layer is very important as the whole system is built around the data received by this layer. The security in the perception layer is directly dependent on the type of protection and different types of attacks which can affect this layer [26]. IEEE 802.15.4 standard is used along with the security modes available, as shown in Table 4. The security modes can be used to establish confidentiality, Data Authenticity and Integrity.

Table 4: Comparison of application layer protocols with their respective features [23, 24]

Protocols	Features						
	Transmission Type	*Architecture*	*Security*	*Quality of Service*	*CPU/ Memory usage*	*Real Time Applications*	*Header size (bytes)*
CoAP	UDP	Request/ Response	Yes	Yes	Low	Yes	4
MQTT	TCP	Publish/ Subscribe	Yes	Yes	Low	No	2
AMQP	TCP	Publish/ Subscribe	Yes	Yes	High	No	8
XMPP	TCP	Request/ Response Publish/ Subscribe	Yes	No	High	Yes	-

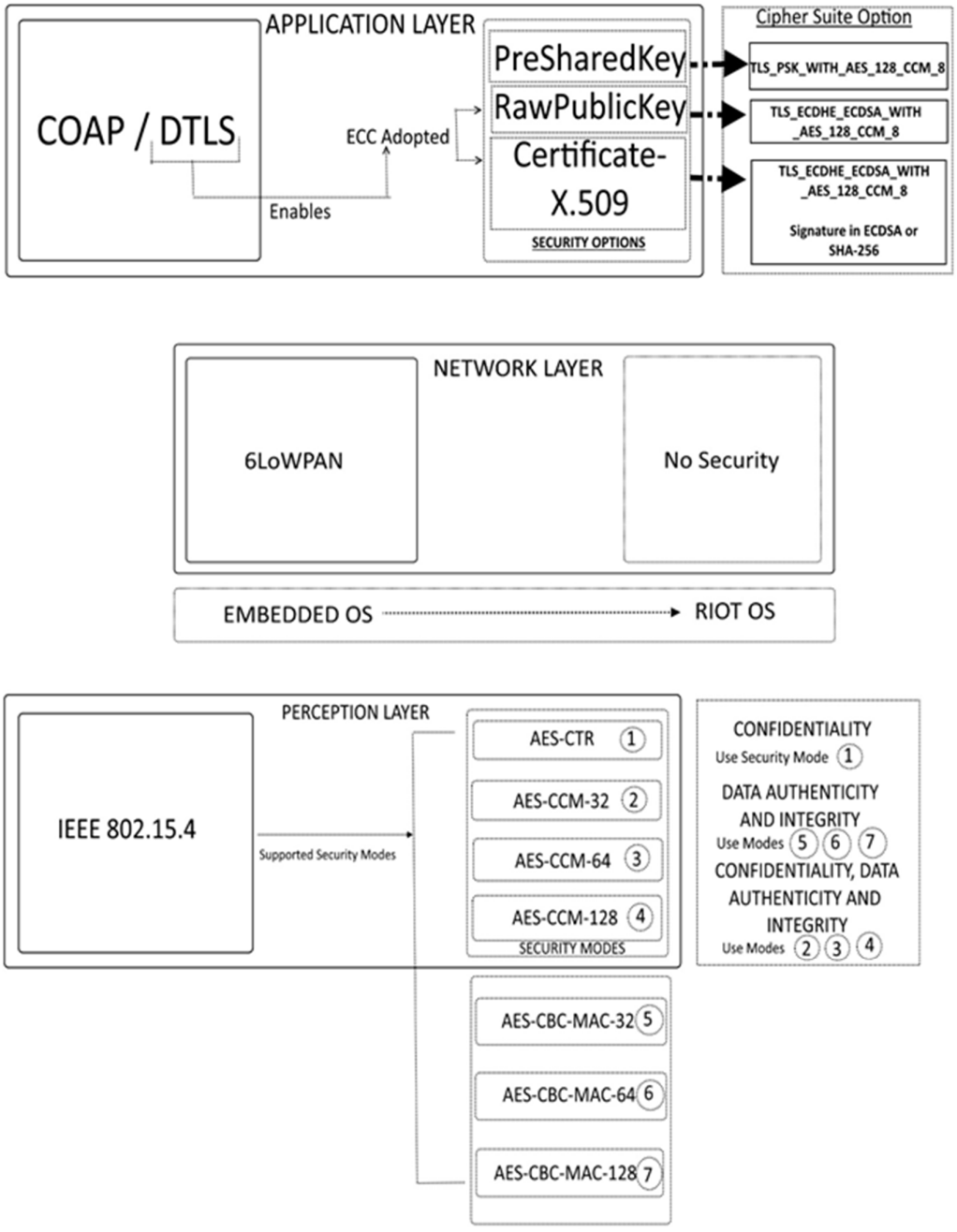

Fig. 5. A framework for IoT Security based on reference [25]

Figure 5 illustrates how they can be grouped together The perception layer is also often known as the "Recognition Layer" and is often regarded as the brain of a conventional IoT architecture.

Under the Network layer, RIOT OS is selected as the embedded OS due to its security features and performance in constraint devices to its security features and performance in constraint devices.

Network Layer: Network layer uses IPv6 over 6LoWPAN and currently does not have any built-in security mechanisms. However, security could be inherited from the stacks provided in the recommended embedded OS, in this case, RIOT OS.

Recommended Framework: The framework is recommended for constrained IoT devices based on their security challenges.
The concept has been demonstrated in Figure 5. It is built on the three layers of IoT; Application, Network and Perception layers

V. Conclusion and Future Work

In this paper, the current state of IoT security and privacy issues has been discussed. Different layers of the IoT are studied, including network, perception and application layer, which gave an overall perspective of the protocols and security related to these layers. Several IoT architectures are studied to give an insight to how the layers are stacked to improve security. Major security requirements, challenges and solutions have been identified via literature review. A framework to provide security on three layers; network layer, application layer and perception layer was recommended.

Designing an intelligent system is an interesting and challenging undertaking that has attracted the attention of many researchers. Concepts like ontologies, agents and semantic web have been thought of to improve the interoperability among different devices of different specifications.

Future work involves further improving the effectivity of the proposed model against threats and to expand the model to cover other vulnerable areas so that the interoperability can be achieved with enhanced security and privacy measures.

References

[1] A. Ahmed, M. M. Parvez, M. M. R., M. H. Hasan, F. N. Nur, N. N. Moon, A. Karim, S. Azam, B. Shanmugam and M. Jonkman, "An Intelligent and Secured Tracking System for Monitoring School Bus," *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019.

[2] J. Pescatore, "Securing the Internet of Things survey," *A SANS Analyst Survey* [Online], 2014.

[3] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 461–491, Jan. 2004.

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

[5] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018. doi:10.1016/j.jisa.2017.11.002.

[6] M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," 2017 *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017.

[7] V. Hovsepyan, "Securing data transfer in IOT environment," *Ukrainian Scientific Journal of Information Security*, vol. 22, no. 2, 2016.

[8] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[9] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[10] B. Chung, J. Kim, and Y. Jeon, "On-demand security configuration for IoT devices," 2016 *International Conference on Information and Communication Technology Convergence (ICTC)*, 2016.

[11] A. Gai, S. Azam, B. Shanmugam, M. Jonkman, and F. D. Boer, "Categorisation of security threats for smart home appliances," *Int. Conf. on Computer Communication and Informatics,* 2018.

[12] B. Fabian and O. Gunther, "Distributed ONS and its Impact on Privacy," 2007 *IEEE International Conference on Communications*, 2007. doi:10.1109/icc.2007.207.

[13] E. Grummt and M. Müller, "Fine-Grained Access Control for EPC Information Services," *The Internet of Things Lecture Notes in Computer Science*, pp. 35–49, 2008.

[14] T. Musa, K. C. Yeo, S. Azam, B. Shanmugam, A. Karim, F. N. Nur and F. Faisal, "Analysis of Complex Networks for Security Issues using Attack Graph," *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019.

[15] F. H. Semantha, S. Azam, K. C. Yeo, and B. Shanmugam, "A Systematic Literature Review on Privacy by Design in the Healthcare Sector," Electronics, vol. 9, no. 3, p. 452, Jul. 2020.

[16] R. T. Tiburski, L. A. Amaral, E. D. Matos, and F. Hessel, "The importance of a standard security architecture for SOA-based iot middleware," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 20–26, 2015.

[17] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based iot: challenges, countermeasures, and future directions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[18] A. Dvir, T. Holczer, L. Buttyan, "VeRA - version number and rank authentication in RPL," In: 2011 *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pp. 709–714, 2011.

[19] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," In: *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2013*, pp. 55–66, 2013.

[20] A. Arış, S. F. Oktuğ, and T. Voigt, "Security of Internet of Things for a reliable Internet of services," *Lecture Notes in Computer Science Autonomous Control for a Reliable Internet of Services*, pp. 337–370, 2018. doi:10.1007/978-3-319-90415-3_13.

[21] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.doi:10.1016/j.jnca.2017.04.002.

[22] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2012.

[23] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017.

[24] M. B. Yassein, M. Q. Shatnawi, and D. Al-Zoubi, "Application layer protocols for the Internet of Things: A survey," 2016 *International Conference on Engineering & MIS (ICEMIS)*, 2016.

[25] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, 2015.

[26] K. Zhao, & L. Ge, "A survey on the Internet of Things security," *9th Int. Conference on Computational Intelligence and Security*. IEEE, 2013.

[27]. A. Kathed, S. Azam, B. Shanmugam, A. Karim, K. C. Yeo, F. D. Boer, and M. Jonkman, "An Enhanced 3-Tier Multimodal Biometric Authentication," *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019.

[28] R. Shokeen, B. Shanmugam, K. Kannoorpatti, S. Azam, M. Jonkman, and M. Alazab, "Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things," *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 2019.

[29] E. Ahmed, A. Islam, F. Sarker, M. N. Huda, and K. Abdullah-Al-Mamun, "A road to independent living with smart homes for people with disabilities," *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)*, 2016.