Security Considerations in the Internet of Things Protocol Stack

Kishor Krishnan Nair[1] and Harikrishnan Damodaran Nair[2]
[1] Defense and Security Centre, Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2] Cochin University College of Engineering Kuttanad (CUCEK), Kerala, India
Email: knair@csir.co.za

***Abstract*—Internet of Things (IoT) wireless devices has the capability to interconnect small foot-print devices and its key purpose is to have seamless connection without operational barriers. It is built upon a three-layer (Perception, Transportation, and Application) protocol stack architecture. A multitude of security principles must be imposed at each layer for the proper and efficient working of various IoT applications. In the forthcoming years, it is anticipated that IoT devices will be omnipresent bringing several benefits. The intrinsic security issues in conjunction with the resource constraints in IoT devices enables the proliferation of security vulnerabilities. The absence of specifically designed IoT frameworks, specifications, and interoperability issues further exacerbates the challenges in the IoT arena. This paper conducts an investigation on IoT wireless security with a focus on the major security challenges and considerations from an IoT protocol stack perspective. The vulnerabilities in the IoT protocol stack are laid out along with a gap analysis, evaluation, and the discussion on counter-measures. At the end of this work, critical issues are highlighted with the aim of pointing towards future research directions and drawing conclusions out of it.**

Keywords- Internet of Things (IoT); IoT Protocol Stack; Security; Vulnerability; Wireless.

I. INTRODUCTION

IN 1999, the initial idea of IoT and its terminology was devised by Kevin Ashton [1]. The rationale for the coneptualisation of IoT was to facilitate the connectivity of "things" (devices). "It is projected that there will be approximately 20 billion interconnected IoT wireless devices with an anticipated data exchange rate that is in the range of 40 Zettabytes towards the end of 2020" [2, 3]. Moreover, it is predicted that it is going to revolutionise and may lead to industrial and commercial sectors [4]. The IoT paradigm masks a significant trial amplified by the absence of specifications specifically designed for resource constrained devices [5]. In addition, IoT devices due to its critical vulnerabilities, exemplify a favorable environment for the current security issues.

In 2016, Distributed Denial of Service (DDoS) attacks were launched against the Domain Naming System (DNS) service provider Dyn. During this attack, a significant amount of vulnerable IoT devices were infected by the Mirai malware. As per the security experts, this attack has been the largest DDoS attack recorded, with an estimated payload of 1.2 terabits/second [2]. Furthermore, during the same period, cyber security experts discovered a flaw in the Zigbee radio protocol [3]. It was showcased using a drone that targeted a series of smart light bulbs infecting them with a malware that triggered the lights on and off continuously. This malware was also able to propagate to neighboring devices.

The remaining sections of this paper is structured as follows: Section II discusses in detail the IoT protocol stack and Section III looks into IoT security. Section IV conducts a GAP analysis and evaluation of IoT security. Section V focuses on the future direction and Section VI concludes this work.

II. IOT PROTOCOL STACK

The IoT protocol stack is divided into three layers. They are the Perception, Transportation, and Application layers. These layers are further described as follows [7, 10]:

A. Perception Layer: This layer is the physical layer of the IoT devices. It senses and acquires data. And it deals with the collection of IoT data and processing in various domains. IoT devices such as extenders are used to perform various measurements and functionalities during the data collection process. The key purpose of this layer is to assimilate the physical attributes of the devices that form the basis of the IoT ecosystem.

B. Transportation Layer: This layer offers a foundation and a prevalent operating setting for the perception layer. The key task of this layer is to route the information acquired from the perception layer to various data processing systems through data communication infrastructures.

C. Application Layer: The application layer serves the end users. It offers different sets of measurements to the end users that are in need of such type of information. The significance of this layer is that, it has the capability to offer smart services to accomplish various end users' demands and requirements.

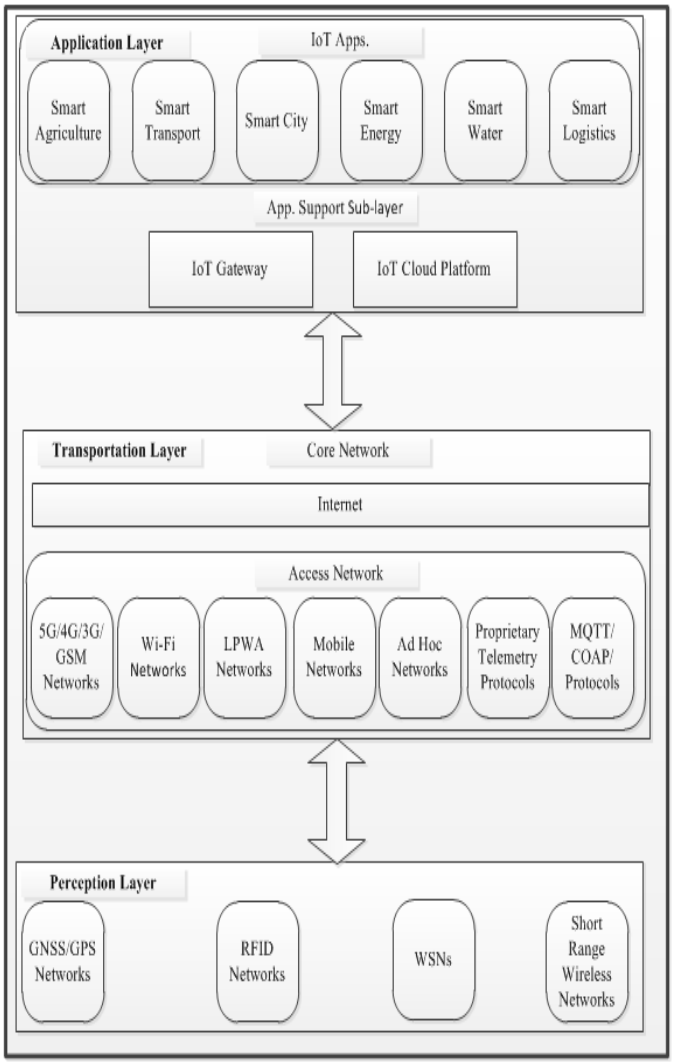

Fig. 1 IoT Protocol Stack Architecture [6]

A general IoT Protocol Stack architecture based on a layered approach is illustrated as above in Fig. 1. The perception layer performs data collection functionalities using various technologies such as Global Navigation Satellite Systems (GNSS)/Global Positioning Systems (GPS), Radio Frequency Identifiers (RFID), Wireless Sensor Networks (WSNs), and Short Range Wireless Networks (such as Zigbee and Bluetooth) [7]. The transportation layer is responsible for communications, routes the data to the application layer using access networks such as 5G/4G/3G/Global System for Mobile Communication (GSM), Wi-Fi, Low Power Wide Area Network (LPWAN) (such as NB-IoT and LoRa), mobile networks, Ad Hoc networks, proprietary telemetry protocols and Constrained Application Protocol (CoAP)/ Message Queue Telemetry Transport (MQTT) protocols [7, 8]. The application layer takes care of the logic, interfaces, syntax, and semantics based on which the IoT applications are built upon [7]. Each layer in the protocol stack offers its own specialised functionality that cannot be replaced by no additional layer. And the individual layers are deemed essential and improvements in these layers are necessary to address various security vulnerabilities [7].

III. IoT Security Challenges and Considerations

The IoT security challenges in general differ vastly from the conventional computing platforms such as Personal Computers (PCs), laptops, and tablets. IoT devices has unique constraints and Table I illustrated below summarises the foremost security challenges that are typical to IoT environment [4. 6, 9, 10, 11].

TABLE I.
KEY IoT SECURITY CHALLENGES

Security Challenges	**Brief Description**
Unattended devices	These devices are designed to work without any user interaction. In these devices, a security compromise might live for a significant period of time before being attended to.
Unmanaged devices	Majority of the IoT devices are created without crucial design considerations with a view of possible upgrades that are required in the future. These mechanisms may not be practical for resource constrained devices. Furthermore, the identified issues in one of these devices will permanently be their if the full batch of devices are not recalled.
Constrained devices	Majority of the IoT devices, due to resource limitations, may not offer the exact level of security that are expected from conventional computing platforms. Power requirements are stringent for IoT devices along with battery life, processing speed, and bandwidth. This confines the choice of counter-measures, such as cryptography.
Massive deployments	IoT devices are usually deployed in a massive scale. Therefore, conventional methods and infrastructure requires additional deliberations.
Identical devices	Identical or near identical devices manufactured by different IoT vendors exacerbates the potential vulnerability in one of the device models.
Long lifespan	Many of the IoT devices especially the LPWAN devices typically have a life span in the range of 12 to 15 years. The security mechanism may not be enough for the full life span and moreover, the security updates, maintenance and support are also huge challenges.
Cross device dependencies	IoT devices can communicate with its peer devices through external communication ecosystems. This requires dynamic and composite cross device dependencies.
Wireless communications	Majority of the communication technologies used by the IoT are of wireless nature. The wireless communication devices are of broadcast nature and therefore an attacker can easily record, alter, replay and relay the altered packets into the wireless communication network.
Physical accessibility	IoT devices are commonly operated in environments where the physical security is a challenge. An attacker who compromises the device can plant a plethora of attacks that are difficult to plant on devices from a remote location.
Newly connected devices	Systems that are designed initially to work in isolation may be upgraded to work with other systems. Thus, connectivity needs stringent security requirements and this becomes a challenge during device migrations.
Cyber Physical Systems (CPS)	IoT devices can affect the CPS, triggering probable attacks that may have greater impact than purely virtual attacks.

Table II illustrated below captures the key vulnerabilities in the IoT protocol stack [9, 10, 11].

TABLE II.
VULNERABILITIES IN IOT PROTOCOL STACK

Protocol Layer	**Key Vulnerabilities**
Application	Malicious code injection
	Information leakage
	Sniffing attack
	Phishing attack
	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attcks
Transportation	DoS and DDoS attacks
	Routing attacks
	Data in Transit (DiT) attacks
Perception	Physical/Hardware level attacks
	Impersonation
	Side-Channel attacks
	False data injection attacks
	Interference/ Eavesdropping attacks
	Sleep deprivation vulnerabilities
	Booting vulnerabilities
	Hardware/Software exploitation
	Tampering of node
	DoS/DDoS attacks
	Routing attacks
	Data in Transit (DiT) attacks

The vulnerabilities highlighted in Table II are explained as follows [9, 10, 11]:

- Malicious code injection: In this, attackers injects malicious codes through identified loop holes, resulting in additional application level infections.
- Information leakage: In this, attackers can compromise and obtain data by well-known vulnerabilities of the application under consideration.
- Sniffing attack: In this type, the attacker could gain network information typically through a sniffing application. This will compromise the security in the system and its transportation layer, which will then lay the foundation for a sniffing attack.
- Phishing attack: In this case, typically emails are used to plant this attack. The emails will be essentially having hyperlinks to a back-door. The attacker gains credentials of the victim and damage data once the victim accesses the hyperlinks.
- DoS/DDoS attacks: attackers can make use of the constrained processing capability of the nodes, making them inaccessible by flooding with heavy data payloads in most of the cases.
- Routing attacks: the attacker alters intermediate malicious node's routing paths during routing and data accumulation.
- DiT attacks: various security breaches on the confidentiality and integrity occur during data transit such as the Man-In-The-Middle (MiTM) attacks.
- Physical/Hardware level attacks: In these attacks, the attacker needs to be in the near proximity with in the IoT devices for the attacks to succeed.
- Impersonation: identification and verification in the IoT scenario is very cumbersome, which may lead to impersonation attacks using fake identity tokens.
- Side-Channel attacks (SCA): in this case, various permutations of SCA based on various parameters such as frequency, power-consumption are devised to compromise the keys used for ciphering or deciphering of sensitive data.
- False data injection attacks: an attacker can broadcast corrupted data through a compromised node. This can lead to unexpected series of events during a service delivery to the service recipient.
- Eavesdropping and Interference: attackers can eavesdrop or sniff the communication channel both wired and wirelessly to obtain sensitive transaction data. Attackers can also spawn DDoS/DoS attacks by injecting noise during data exchange.
- Sleep deprivation attacks: this attack is usually executed by draining out critical device resources such as the battery connected to devices in the perception layer. Hardware tampering or malicious code injection can upsurge the power ingestion of the device. This can then lead a complete drainage of the device battery.
- Booting vulnerabilities: During the device startup, typically majority of the security mechanisms are not enabled and an attacker with an effort can well access device and application configuration files to obtain the secret keys and can ultimately compromise the device.
- Hardware exploitation: attacker can compromise the device through its hardware peripherals. This attack is performed by sophisticated test terminals which injects malicious code into the device that accesses hardware peripherals and device ports.
- Software vulnerabilities: software vulnerabilities in IoT are analogous to the conventional computing platforms such as laptops and tablets. Application architecture designed for IoT are very much on par with these systems and therefore the security issues applicable to them are equally applicable to IoT also.
- Tampering of node: attacker can typically tamper and IoT node to compromise the device and modify sensitive data such as the device configuration files.

IV. GAP Analysis and Evaluation of IoT Security

Fig. 2 below illustrates a Security Expectations Pyramid in IoT. As illustrated in the figure, each rectangular block captures key security features that are expected to be fulfilled by IoT devices and IoT applications in general. However, in majority of the IoT security contexts, this is not the case. This section attempts to conduct a GAP analysis and evaluation of IoT security.

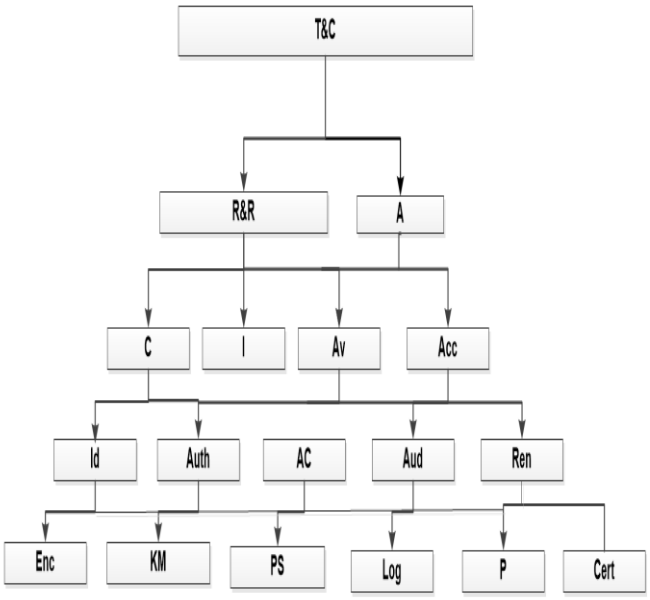

Fig. 2 Security Expectations Pyramid in IoT

The labels in Fig2. corresponds to the following: T&C: Trust and Confidence, R&R: Rights and Responsibilities, A: Assurance, C: Confidentiality, I: Integrity, Av: Availability, Acc: Accountability, Id: Identification, Au: Authentication, AC: Access Control, Aud: Auditing, Ren: Renewability, Enc: Encryption, KM: Key Management, PS: Platform Security, Log: Logging, P: Patching, Cert: Certification

The GAP analysis takes into consideration the baseline security requirements and the target security requirements. Furthermore, it identifies the security building blocks between the baseline and the target. The key baseline security requirements are attributed to the Confidentiality, Integrity and Availability (CIA) [9]. However, IoT has challenges in terms of the device capabilities and configurations. Moreover, additional constraints such as restricted computational and power resources of IoT also needs to be taken into consideration. The key target security requirement is to ensure security across all IoT protocol stack layers. And at the same time, the target security should also include a holistic security of the entire value-chain [10].

The challenges in IoT devices are classified into two streams. They are the security challenges and the technological challenges [11]. Security challenges entail the ability to safeguard security in terms of authentication, confidentiality, authorisation, end-to-end security, and data integrity. The security challenges are related to the policies, procedures, and protocols that should be imposed to achieve a safe and secure network. Technological challenges are attributed to the underlying wireless communication technologies that the IoT device forms part of. The technological challenges creep up due to the pervasive and diverse landscape of IoT devices [12]. Security must be prescribed in the full value chain of IoT devices [11].

In the conventional communication protocols, the nodes are interlinked using physical mechanisms. Where as IoT devices relies on wireless networks for end to end communications. IoT networks are at risk due to the broadcast transmission nature of its protocols and network topologies [7]. IoT devices are prone to the security vulnerabilities due to the weakness in various layers of the underlying protocol stack. Ciphering/deciphering methods assume that the attacker has inadequate competences in resources and skills. And believes and trust on the computational toughness of their principal mathematical algorithms. Data generated by IoT devices are either kept in the devices itself or is broadcasted over the networks such as the Internet. IoT inherently is exposed as the devices in most instances exchange data over unrestricted domains. Therefore, in order to protect the data, CIA as depicted in Fig. 2 must be provided at a bare minimum. Adequate security checks and mitigations must be put in place to offer one or more of these defense mechanisms. Furthermore, the vulnerabilities and threats are measured in terms of their ability to thwart the CIA principles.

Majority of the IoT devices are packaged and configured in such a way that one cannot add security features at a later stage once the devices have been released from the Original Equipment Manufacturer (OEM) outlet and this opens the door for a plethora of security vulnerabilities. Due to this, security has to be incorporated into IoT devices during manufacturing to make them inherently secure. This needs to be changed and the security concept must mature from default security to add-on security such as the one's that we use at the moment for the existing platforms such as laptops, and PCs.

Currently, IoT wireless devices, only support lightweight algorithms and in most cases compromising security to cater for lower device capabilities. In the near future it is anticipated that there will be different flavors of IoT devices potentially connecting to the web, from sophisticated IoT enabled automobiles to wearables. These diverse devices, running on various IoT protocols are anticipated to generate huge volumes of miscellaneous data along with a variety of new security threats.

The exponential increase in the vulnerability landscape in IoT devices leads to a ripple effect in IoT security. In the IoT protocol stack, it is highly difficult to prevent attacks on the perception layer. This is due to the following factors: 1) in majority of the cases the perception layer is open and exposed and due to this, the security mechanisms used in the closed environment will not work well in open environments and 2) technological heterogeneity determines difficulty of using only one kind of security technology [6]. In the transportation and application layer, privacy violations are more predominant as IoT applications are used in one's daily life. Moreover, these devices collect private information in huge volumes in an automated fashion for various use cases. In fact, certain IoT use cases can even control one's home environment and this can lead to serious security breaches [6]. Table III depicts the evaluation of the IoT wireless security based on the information collected from various IEEE research articles [6, 12, 13, 14, 15, 16, 17, 18, 19, 20].

To tackle the vulnerabilities listed in Table III, the protocol layers and interfaces of IoT system needs to be secured in general to make sure that the expected security requirements are met in general. In the perception layer, the commonly used technologies to communicate wirelessly are LPWAN technologies such as LoRa, Sigfox, NB-IoT, and Zigbee. The predominant security challenges that are in the perception layer are compromise of node authentication and confidentiality of information. Attacks such as DDoS and weak physical security coupled with insecure installation and configuration of IoT devices brings along a separate set of new vulnerabilities.

Recently, security in perception layer is gaining a lot of traction. It is evolving as an appropriate means of securing communications in wireless protocols to achieve a promising and a robust level of security against security attacks. Perception layer level encryption/decryption exploits the security techniques that are applicable in the baseband wireless channel. And the mitigation measures in the perception layer are in terms of Black network solution, AES-CCM algorithms, WEP/WPA/ WPA2 protocols, and EEA/EIA algorithms.

TABLE III.
EVALUATION OF IOT SECURITY

Protocol Layer	**Wireless Protocol**	**Security Vulnerability**	**Counter-measures**
Perception Layer	LPWAN, BLE, Wi-Fi, LTE, IEEE 802.15.4	Malicious attacks, Spoofing, Data Transit Attacks, Eavesdropping, MITM attacks, message falsification/ injection attacks,	Black network solution, AES-CCM algorithms, WEP/WPA/ WPA2 protocols, EEA/EIA algorithms
Transportation Layer	IPv4/IPv6, LTE, Wi-Fi, LPWAN, IEEE 802.15.4	MITM attacks, counterfeit attacks, data congestion, Data Transit Attacks, Threats to NDP protocol, DoS and Routing attacks	DTLS protocol, IPsec and Compressed IPsec protocol, SEND protocol in IPv6, 802.15.4 security features, SVELTE IDS solution, AES/CCM algorithms
Application Layer	MQTT, COAP	High hand shake of DTLS, Data Transit Attacks, Heavy computation cost of TLS, Scalability issues in Key Management	Secure MQTT solution with ABE, TLS with PSK/Certificates, SecKit solution, DTLS protocol with PSK/RPK certificates, Lithe solution

In the transportation layer, security attacks like the MiTM and cloning attack are experienced along with data congestion and other security vulnerabilities. The major protocols used in this layer are IPv4/IPv6, Wi-Fi, LTE, LPWAN, and IEEE 802.15.4. As perception layer and transportation layer works hand in hand, vulnerabilities such as compromising devices using unsafe services are most prevalent. Furthermore due to lack of transport layer encryption and insufficient authentication, cloud interface attacks and malicious information attacks are also quite common in this layer [9].

The counter-measures proposed by various researchers in the Transportation layer includes DTLS, IPsec/Compressed IPSec protocols, and SEND protocol used in IPv6. Moreover, 802.15.4 security features, SVELTE IDS solution, and AES/CCM algorithms are also used in Transportation layer security.

The foremost application layer protocols used in IoT are MQTT and CoAP. In the application layer, privacy and security protection in terms of data sharing plays a major role. The major counter-measures proposed to mitigate application layer vulnerabilities are Secure MQTT solution with ABE, TLS with PSK/Certificates, SecKit solution, DTLS protocol with PSK/RPK certificates, and Lithe solution.

V. Future Direction

Future research can be performed to propose a dynamic and an automated IoT security framework into the current IoT protocol stack. Furthermore, future research can look into security schemes and policies that can be incorporated in the framework to identify and mitigate vulnerabilities on the fly. Another research direction that can be significantly reconnoitered will be to secure the inter domain data communications and access control between various IoT devices. The aim here will be to facilitate the necessary interoperability between IoT devices.

VI. Conclusion

Based on the existing IoT protocol stack architecture, this research laid out the key security challenges and vulnerabilities from the perception layer, transportation layer, and application layer respectively. This was followed by a GAP analysis and evaluation of the IoT security protocol stack with counter-measures. And through the GAP analysis and evaluation of IoT security, it is learned that the IoT device security is frequently overlooked or considered as an overhead by the OEMs and IoT device vendors. This is primarily due to the time available to launch the product to market. Furthermore security is omitted in most instances to reduce the cost. This in turn results in the compromise of security features. IoT devices offering minimal security protection in most instances makes use of software level solutions, such as secure application signing. Usage of software-based protection schemes often leaves the hardware peripherals vulnerable and this indirectly leads to security issues in the protocol stack layers. With the growing usage of IoT devices in every day existence especially in priority real time use cases, the identification of security vulnerabilities and the corresponding counter-measures are extremely important and needs be to carefully considered.

References

[1] S. Gupta, N. Mudgal, and R. Mehta, “Analytical Study of IoT as the Emerging Need of the Modern Era,” 3rd International Conference on Computing for Sustainable Global Development, New Delhi, India, pp. 233-235, 2016.

[2] Gartner, “Gartner says 6.4 billion connected “things” will be in use in 2016, up 30 percent from 2015,” Online: http://www.gartner.com/newsroom/id/3165317, Last Accessed 08/10/2018.

[3] Forbes, “152,000 smart devices every minute in 2025: Idc outlines the future of smart things,” Online: http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#34bf983369a7, Last Accessed 08/10/2018

[4] A.H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q.Z. Sheng, “IoT Middleware: A Survey on Issues and Enabling Technologies,” IEEE Internet of Things Journal, vol. 4, no. 1, 2017

[5] K. Nair, E. Dube, S. Lefophane, “Modelling an IoT Testbed in Context with the Security Vulnerabilities of South Africa,” 3rd IEEE International Conference on Computer and Communications, Chengdu, China, pp. 244-248, 2017.

[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), IEEE, Helsinko, Finland, ISBN. 978-1-5386-3070-9 2017

[7] H. A. Khattak, M. A. Shah, S. Khan,I. Ali, M. Imran, “Perception layer security in Internet of Things,” Future Generation Computer Systems, ELSEVIER, vol. 100, pp. 144-164, 2019.

[8] K. Nair, A.M. Abu-Mahfouz, and S. Lefophane, “Modelling an IoT Testbed in Context with the Security Vulnerabilities of South Africa,” 2019 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, ISBN. 978-1-5386-7365-2, 2018.

[9] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan , "Internet of things (IoT) security: Current status, challenges and prospective measures", 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, ISBN.978-1-9083-2052-0, London, UK, 2015

[10] B.V.S. Krishna and T Gnanasekaran, “A systematic study of security issues in Internet-of-Things (IoT),” 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, ISBN.978-1-5090-3243-3, Palladam, India , 2017

[11] P. N. Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things", J. of Cyber Security and Mobility, vol. 1, pp. 309-348, 2013

[12] M. Leo, F. Battisti, M. Carli, A. Neri, "A federated architecture approach for Internet of Things security", Euro Med Telco Conference (EMTC), pp. 1-5, 2014.

[13] N. S. Labib, M. R. Brust, G. Danoy, P. Bouvry, "Trustworthiness in IoT – A Standards Gap Analysis on Security, Data Protection and Privacy",ISBN.978-1-7281-0864-3, DOI.10.1109/CSCN.2019.8931393, 2019

[14] E. Carpentier, C. Thomasset, J. Briffaut, "Bridging The Gap: Data Exfiltration In Highly Secured Environments Using Bluetooth IoTs", ", ISBN. 978-1-5386-6648-7, DOI. 10.1109/ICCD46524.2019.00044, 2019

[15] R. Shokeen, B. Shanmugam, K. Kannoorpatti, S. Azam, M. Jonkman, M. Alazab, "Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things", ", ISBN. 978-1-7281-2601-2, DOI. 10.1109/CCC.2019.00-14, 2019

[16] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. Abbas, "An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security", IEEE Internet of Things journal, DOI. 10.1109/JIOT.2020.2997651, 2020.

[17] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems", ISBN. 978-1-7281-2171-0, DOI. 10.1109/GIOTS.2019.8766407, 2019

[18] K. Nair, M.M. Pillai, S. Lefophane, H.D. Nair, "Adaptation of Smart Cities in the South African Internet of Things Context", ISBN., DOI., 2020

[19] M. M. Hossain, M. Fotouhi, R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", ISBN. 978-1-4673-7275-6, DOI. 10.1109/SERVICES.2015.12, 2015

[20] I. Nakagawa and S. Shimojo , "IoT Agent Platform Mechanism with Transparent Cloud Computing Framework for Improving IoT Security", ISBN. 978-1-5386-0367-3, DOI. 10.1109/COMPSAC.2017.156, 2017