An Insight into Current IoT Security Methods

K.K. Yuen, W.H. Shim, T.T. Ting and C.K. Teoh
Tunku Abdul Rahman University College.
tingtt@acd.tarc.edu.my

***Abstract*—This paper examines the security methods in the Internet-of-Things. The security methods are carefully studied and categorized into six layers according to the Internet-of-Things framework namely Event Producer and Consumer, Event Queuing System, Transformation and Analysis, Storage, Presentation and Action, and Users and Systems. It can be observed that most security methods emphasizes on Event Producer and Consumer layer whereas the least focused layer is Users and Systems layer. This study aims to present a comprehensive overview to researchers working in the domain of the Internet-of-Things security.**

***Index Terms*—Framework; Internet-of-Things; Protocol; Security.**

I. INTRODUCTION

The Internet-of-Things (IoT) is a new era of computing domain which utilizes technologies such as Radio Frequency Identification (RFID), sensor network and cloud computing technology. Cloud computing provides virtual infrastructures that allows the integration of various monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. In addition to providing end-to-end service, it also enables users to access their application and devices across time and space.

There are few stages involved in the transfer of data from the beginning to the end such as data initialization, data collection, data organization and data storage. In data initialization, the event is detected by the sensors present in smart devices. Every event is encapsulated in a packet of data and sent over the network using lightweight communication protocols such as MQTT, HTTP, and CoAP which is consolidated at a central broker. These protocols are the most common standard protocols adopted in IoT devices. After the data is sorted based on its respective topic, it will be sent to the database for further use.

Figure 1 describes the IoT framework which consists of six layers namely Event Producer and Consumer, Event Queuing System, Transformation and Analysis, Storage, Presentation and Action, and Users and Systems. The following sub-sections will discuss the layer of data transmission between databases to the presentation, followed by the categorization of existing IoT security methods into the various six layers of IoT framework.

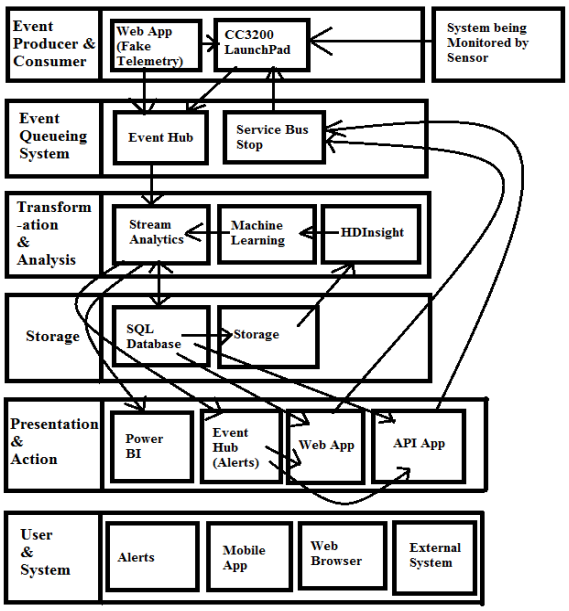

Figure 1: IoT framework based on Glenn [15]

.

II. DATA TRANSMISSION BETWEEN DATABASES TO PRESENTATION

Data transmission from database to presentation presents numerous security issues such as unauthorized data access and modification and the risk of data breaches which poses a critical risk of compromising the confidentiality of information stored [3]. For example, the graphs that are present in (Microsoft Azure) Event Hub will not be presented consistently; fitted curves will be erroneous, which in turn leads to various uncertainties and misleading information [25]. To resolve these issues, network protocol plays a crucial role in encrypting every key data that are in the process to be sent to the communication section, where database records communicate with presentation methods to be converted into presentable information such as graphs and charts [25]. Lookup tables are used to identify its source and destination nodes, greatly decreasing the risk of other unauthorized accesses with ease and results in a significant reduction of unauthorized data modification [3, 25].

Network Protocols are used when messages are in the process to be sent to the Communication section, where it enters the network gateway. It uses Tunneled Agile Routing Protocol (TARP), a highly secured mechanism which consists of "*double layer encryption format and special routers*" [28]. The normal IP Protocol will then be used to send IP packets which will be exchanged with TARP terminals through the router, hiding the true destination address in the process, which is seen only by the TARP routers and servers. Each encrypted key will then be

generated by a link key to mask it. Its own destination addresses are only made available by the TARP routers and the remaining routers will be restricted from gaining access to it [28]. TARP's IP address can also be changed by utilizing its unique IP agility feature on the Lookup Table (LUT). Suppose, when an IP Address alteration is detected, the address in the rest of the TARP routers and terminals LUT are also altered simultaneously [26].

Threshold sensitive Energy Efficient Network (TEEN) is a protocol that is used for reactive networks such as time critical applications and intrusion detection. TEEN promotes efficiency by limiting the power consumption in the sensor nodes [28]. As a result, the network protocol will be fault-tolerant which greatly enhances reliability and accuracy of the wireless sensors at the gateway. It also communicates with other nodes using Wireless Mesh Networks (WMN) [13, 26, 28].

A. Optimized Link State Routing Protocol

Optimized Link State Routing Protocol (OLSR) is developed primarily for mobile ad-hoc networks. It can overcome traffic flood by making use of Multipoint Relays (MPR) to reduce the number of transmissions to maintain a sustainable traffic control [6]. MPR declares a unique link state information in the network, which enables OLSR to provide the shortest path route. Quality of Service (QoS) is a prefixed agreement that provides either the qualitative or quantitative type of metric standards [6] or OLSR complements QoS components in choosing one or more network paths to provide sufficient resources such as the information path for admission control in order to have global efficiency. In addition, it can also provide the shortest path since it does not need full link state and support for earlier protocol extensions [6, 14, 20].

B. Better Approach To Mobile Adhoc Networking

Better Approach To Mobile Adhoc Networking (BATMAN) is a dynamic routing protocol designed for WMN. It makes good use of routing metric and distance vector approach which assimilates the reliability of all the radio links. Each node consists of a routing table which stores potential next hops to the rest of the nodes, thus forming WMN [11]. Ad hoc On-Demand Distance Vector Routing (AODV) and BATMAN are suitable to be used in use cases such as a mobile robot traveling along a pre-determined path with three fixed nodes set up along this path. Using the default settings, BATMAN failed to re-establish a route to the controller node after getting out of range for a direct connection.

Every node in BATMAN will broadcast the "*hello"* packets which is known as originator message to its neighbors. Each originator messages consists of an originator address, sending node address and a unique sequence number. Each neighbor changes the sending address to its own address and re-broadcast the message. On receiving its own message the originator does a bidirectional link check to verify that the detected link can be used in both directions. The sequence number is used to check the currency of the message.

BATMAN does not store the full route to the destination since each of the nodes along the route maintains the information for the next link which will then lead to the optimum route [11]. BATMAN is able to locate the best route to the destination using a simple algorithm. Suppose BATMAN wants to send a message from node 1 to node 6. However, node 1 is routed to node 2, 3, and 4. From node 2, the message can be routed to node 5 then 6. On the other hand, node 4 is connected to node 6. Therefore, BATMAN will determine the best link which is node 4. When BATMAN receives a new message (Originator message), each node will store it in a buffer to keep track of the previous message received. Each node will then update the latest time of the reception of the message created, received, or forwarded by this node. The nodes that have the highest number of occurrence denote the shortest route. This will be used to determine the best path to reach the originator [8, 19, 11].

III. EVENT PRODUCER AND CONSUMER

Human-like security immune safeguard will be accomplished when physical security is indicated in an external context and inherent infrastructure [29]. Innate immunity provides a basic barrier against foreign invasion in a real-time environment. This immunity will be triggered if the sensors of intelligent pattern recognition mechanism identify any anomaly attacks. Rejection reactions will be controlled by the management centre whenever a co-stimulation signal is transmitted to different nodes which have distributed control [29]. When the immunity is in defensive operation, the activation thresholds are defined to ensure the detection optimization and fuzzy logic diagnosis will be used to achieve a better detection.

Adaptive immunity refers to acquired resistance, where an attack is marked as a specific signature [29]. If the IoT is attacked or infected by the same attack or invasion, a specific memory module will be triggered to eliminate the damaging effect by generating an improved response to restore the system to a secure state. This immunity also uses the same fuzzy logic diagnosis to detect any attack or invasion. This immunity is similar to an artificial intelligent defensive system which learns overtime over various attack or invasion.

IV. PERCEPTUAL LAYER

The perceptual layer is the layer that collects all kinds of information that can be identified through physical equipment such as RFID reader and sensors. For the security aspect for the perceptual layer, a node authentication is necessary to prevent illegal node access, data encryption for the confidentiality of information transmission between the nodes and prior to a transmission, a data encryption key agreement plays a crucial part in protecting the data transmission in advance [9]. Lightweight encryption technology is also adopted in the perceptual layer to resolve the problem of resource over consumption. This technology includes lightweight cryptographic algorithm and lightweight cryptographic protocol.

Maintaining both the logical and physical security of network facilities and terminal would require a security module to be put in place in the perpetual layer [2]. The base module of the logic security mechanism that is used to protect the perceptual layer consists of encryption mechanism and security algorithm. Authentication of terminal identity to store data confidentiality is enabled through asymmetric and symmetric algorithms [2].

Meanwhile, *hide terminal identity* uses the terminal identity security which manages and destroys the terminal key for fast terminal identification. The Anonymous

algorithm is also used to hide the real identity of the respective terminal. When the user wants to inspect the terminal identity, it will invoke a rollback system function to retrieve the real identity of the terminal.

Another interactive data security is used to ensure that the data generated by the terminal are not interrupted by any unauthorized access. By using the encryption algorithm, it prevents the data being brute-forced, abandoned, replayed while transmitting.

A. Intrusion Detection System

Intrusion Detection System (IDS) monitors the occurrence of network events for any signs of intrusion. It is categorized as a wireless-based solution with three classes which are Signature-based Detection (SD), Anomaly-based Detection (AD), and Stateful Protocol Analysis (SPA). IDS is primarily used to identify three types of event which are Host-based IDS (HIDS), Network-based IDS (NIDS), and Wireless-based IDS (WIDS). It works by using various sensors and agents to collect data via centralized or distributed methodology [23]. All of the collected data types will then be audited. Trails on a host, network packets or connections, wireless network traffic, and application logs cannot supply absolutely accurate detection [10, 12, 17, 21, 23, 27].

B. Radio-Frequency Identification

Radio-Frequency Identification (RFID) uses electromagnetic fields to identify tags (which contain electronic information) which are usually attached to objects. Passive tags collect energy from a nearby RFID reader which constantly transmits interrogating radio waves. The RF voltage which will then be converted to DC current when it receives a signal from the antenna [7, 30]. The current is the power source for the passive RFIDs.

RFID is available with both near and far-field technology. Near field technology applies Faraday's principle which sends data using load modulation through a magnetic field. Once it opposes the reader's field, the small increase in current flow will trigger the set action. On the other hand, far-field technology captures waves that are detected by the reader. The antenna in a far field RFID has precise dimensions which are tuned to a common frequency of 2.45 GHz. If there is a mismatch, it will be detected and reflected to trigger an action.

V. Event Queuing System

An event queuing system is a system that consists of a processor that acts as an event queue which stores tasks and indicates the arrival of event stored in a kernel. Discrete event queuing is one of the scenarios to this system where it determines the arrival of each task based on their inter-arrival and service time [4]. It will then schedule based on the service end time and making way for the next task to arrive. However, security issues that arise will interrupt the event queuing system, which can enable intruders to launch a point attack in the system. These attacks will possibly alter the values which lead to events inaccuracy prior to arrival and departure and slow down the performance. Hence Demilitarized Zone (DMZ) approach is introduced to create a demilitarized zone or a separate zone with stricter security measures in between firewalls. A firewall with DMZ would carry more than 1 layer, which utilizes artificial intelligence such as rule-based knowledge in order to allow for connections of different zones [4]. It is very sensitive to the extent where it checks with the first rule if it matches to the new session. Otherwise, it checks sequentially on the rest until a match is found in the corresponding port numbers [4]. DMZ would sometimes consist of more than one layer. When an intruder passes the initial stage of the firewall, DMZ will block out the access to prevent further intrusion into other firewalls [4, 24].

VI. Storage Layer

Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) are three types of delivery models in cloud computing. Infrastructure as a service (IaaS) is a single tenant cloud layer where the cloud computing vendor's specific resources are only shared with the clients with pay-per-use account. IaaS not only reduces initial investment in computer hardware such as server and networking device but also allows a varying degree of financial and functional flexibility. Resources in computing undoubtedly can be released and added faster, at the same time being cost efficient compared to different data centres and services [31].

Software as a service (SaaS) concept is based on pay-per-use costing model but the model is traditionally accessed remotely using a web browser via the Internet. The functionality of this model is limited and the provider of the SaaS can host their own data centre or host with their co-location providers. Since SaaS is using web browser over the internet, the security of SaaS is dependent on the web browser security. Web Services (WS) security, Extendable Markup Language (XML) encryption and Secure Socket Layer (SSL) are among many options which can be used to secure the data transmitted over the internet.

Platform as a service (PaaS) is a model which is similar to IaaS but PaaS includes a level of pay-per-use functionality. Operational expenses are the costs spent by PaaS service users instead of capital investment. At the same time, additional functionality of layers have additional constraint [31]. The virtual machines that function as a catalyst on the PaaS layer must withstand the attacks such as cloud malware and hacker who maliciously retrieve the business information of cloud user. Therefore, the integrity of application and authentication check during data transfer is crucial. Identification & authentication is a process that verity and validate the cloud user by using their registered username and password protection to protect their cloud profile.

There are few security requirements in the storage layer as follows. Authorization is an information security requirement to ensure referential integrity is maintained [31]. Confidentiality is used to maintain the control of accepted data from different sources over the internet or within the organization databases. Integrity in data access means the due diligence within the cloud domain. Non-repudiation is a process of applying traditional e-commerce security protocols and token provisioning to data transmission within the cloud application [31]. As for all three types of delivery models, Availability is a key decision factor in information security requirement among all the three types of cloud computing (public, private and hybrid). This function highlights the trepidation of availability in cloud service and the resources between cloud computing provider and cloud user.

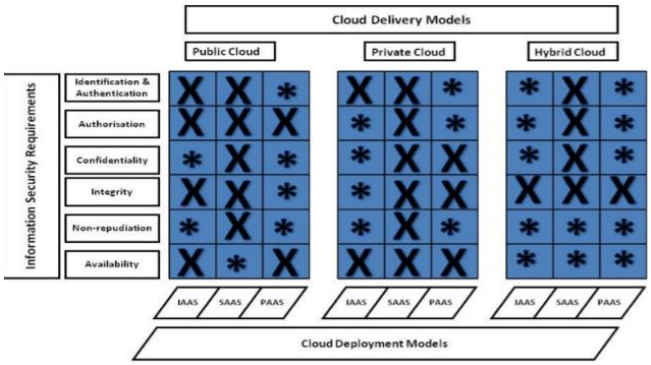

Figure 2: Information security requirements in different types of cloud [31]

In public cloud, Identification & Authentication is required in IaaS and SaaS while Authorization is required in IaaS, SaaS and PaaS. Confidentiality is required in SaaS only and Integrity is required in both IaaS and SaaS. Non-repudiation is required in SaaS, and Availability is required in IaaS and PaaS. Since the public cloud is open to everyone, the security and authority to access are of high concern.

In private cloud, Identification & Authentication is the main concern in IaaS and SaaS. Authorization is required only in SaaS. Confidentiality is required in SaaS and PaaS. Integrity is required in SaaS and PaaS. Non-repudiation is required in SaaS only. Availability is applicable in IaaS, SaaS, and PaaS. This is because the private cloud is only for private use as in personal storage. Therefore, it focuses on identification of data instead of authorization since only the cloud user can access [18].

In hybrid cloud, Identification & Authentication, Authorization and Confidentiality is only required in SaaS. This is because SaaS is based on the web browser. Integrity is required in all SaaS, IaaS, and PaaS because the hybrid cloud is the combination of public cloud and private cloud. Hence, the Integrity must be ensured while combining both platforms. Non-repudiation and Availability are not used in the hybrid cloud.

Based on the aforementioned security requirements, SaaS requires the most features since SaaS is using a traditional access method such as web browser via the Internet, resulting in limited functionality in the protection of data transmission over the Internet [31].

VII. Wireless Sensor Network (Event Producer)

Wireless Sensor Network will connect to the Internet through a gateway with three approaches which are 1. Wireless sensor network connects to the Internet through a single gateway, 2. Few sensor nodes form a hybrid network where the few sensor nodes can connect to the Internet through a gateway, and 3. Multiple sensor nodes connect to the Internet with one hop without a gateway. The sensor nodes play a very important role in ensuring data confidentiality, integrity, availability and authentication depend on the application sensitivity. Should there be any attackers that capture or in an attempt to jam or bring in malicious nodes would require a physical presence near the targeted wireless sensor network [5]. Location proximity will threaten wireless sensor network.

Hence, a wireless sensor network that is connected to the Internet can be protected by a central and unique gateway. The gateway will connect to the Internet provided by a server and accept an incoming connection. Upon receiving the connection, the respective gateway will then forward the received data to the system to undergo evaluation in order to eliminate the possibility of transmission error. By checking extra information such as parity bytes and a predetermined length of incoming data against the real length, mismatched data will immediately be trimmed [5, 16].

VIII. Transformation and Analysis

Machine learning methods are regularly incorporated in the IoT framework to detect system anomaly. It can detect an attack against servers by accumulating system behavior data. Detected abnormal flows are deemed as attacks or intruders. However, some attacks that were launched will have the possibility to destroy the learning algorithm with malicious input which could possibly lead to the machine learning's accuracy where it predicts falsely. As a result, the integrity of the machine learning will be greatly affected and not be as accurate as before [1]. Disproportioned intrusions and exploratory attacks, however, can be easily classified with the aid of training the machine learning with a special set of data [1]. Once successful, these data will further enhance the integrity of machine learning for a reformulation of the algorithm. By acquiring new data and therefore an extra set of training data is required to carry out reformulation [1, 2, 22].

IX. Conclusion

In this study, it can be observed that the works conducted by most researchers incline towards the three layers of the Internet-of-Things framework namely 'Event Producer and Consumer', 'Transformation and Analysis', and 'Storage' which are most vulnerable and prone to exploitation. The least research work lies with the layer of 'Users and Systems'. The underlying reason could be due to the assumption that the security solution in the prior 'Event Producer and Consumer' layer is sufficient in data protection. Albeit the limited works in this layer, there is a possibility that this layer is susceptible to various security breaches.

References

[1] Barreno, Marco, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. Doug Tygar. (2006). Can machine learning be secure? In Proceedings of the 2006 ACM Symposium on Information, computer and communications security. 16-25

[2] Zhang, Weizhe, and Baosheng Qu. (2013). Security Architecture of the Internet-of-Things Oriented to Perceptual Layer. International Journal on Computer, Consumer and Control (IJ3C). Vol.2 No. 2. 37-45

[3] Chen, Deyan and Zhao, Hong. (2012). Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference. Vol 1. 647-651. IEEE.

[4] Cheswick, William.R., Steven M.Bellovin and Aviel D.Rubin. (2003). Firewalls and Internet security: repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc.

[5] Christin, Delphine, Andreas Reinhardt, Parag S.Mogre, and Ralf Steinmetz. (2009). Wireless sensor networks and the Internet-of-Things: selected challenges. Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze. 31-34.

[6] Clausen, Thomas. and Philippe Jacquet. (2003). Optimized link state routing protocol (OLSR). No. RFC 3626.

[7] Want, Roy. (2006). An introduction to RFID technology. IEEE Pervasive Computing. Vol. 5 No. 1. 25-33

[8] Delosieres, Laurent. and Simin Nadjm-Tehrani. (2012). Batman store-and-forward: the best of the two worlds. In Pervasive Computing and

Communications Workshops (PERCOM Workshops). 2012 IEEE International Conference on 721-727. IEEE.

[9] Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. (2012). Security in the Internet-of-Things: a review. In Computer Science and Electronics Engineering (ICCSEE). 2012 International Conference on IEEE. Vol. 3. 648-651

[10] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. (2013). EAACK—a secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics. Vol. 60. No. 2. 1089-1098.

[11] Seither, Daniel, André König, and Matthias Hollick. (2011). Routing performance of Wireless Mesh Networks: A practical evaluation of BATMAN advanced. In Local Computer Networks (LCN). 36th Conference IEEE. 897-904.

[12] Scheidell, Michael. (2009) Secnap Networks Security, LLC. Intrusion detection system. U.S. Patent 7,603,711.

[13] Fielding, Roy, Jim Gettys, Jeffrey Mogul, Henrik Frystyk, Larry Masinter, Paul Leach and Tim Berners-Lee. (1999). Hypertext transfer protocol--HTTP/1.1 .No. RFC 2616.

[14] Ge, Ying, Thomas Kunz, and Louise Lamont. (2003). Quality of service routing in ad-hoc networks using OLSR. In System Sciences. Proceedings of the 36th Annual Hawaii International Conference on 9. IEEE.

[15] Glenn Vassallo. (2015). Code Project. [ONLINE] Available at: https://www.codeproject.com/Articles/890430/Microsoft-Azure-plus-TI-CC-LaunchPad-End-to-End-Io. [Accessed 17 November 2016].

[16] Ha, Minkeun, Kim, Seong Hoon Kim, Hyungseok Kim, Kiwoong Kwon, Nam Giang, and Daeyoung Kim. (2012). Snail gateway: Dual-mode wireless access points for wifi and ip-based wireless sensor networks in the Internet-of-Things. In 2012 IEEE Consumer Communications and Networking Conference. CCNC. 169-173. IEEE.

[17] Horng, Shi-Jinn., Ming-Yang Su, Yuan-Hsin Chen. Tzong-Wann Kao. Rong-Jian Chen.Jui-Lin Lai . and Citra Dwi Perkasa. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert systems with Applications. Vol. 38. No. 1. 306-313

[18] JAMES, BD. (2010). Security and privacy challenges in cloud computing environments.

[19] Johnson, David, Ntsibane Ntlatlapa, and Corinna Aichele. (2008). Simple pragmatic approach to mesh routing using BATMAN.

[20] Wu, Kui, and Janelle Harms. (2001). QoS Support in Mobile Ad-Hoc Networks". Crossing Boundaries – an Inter Disciplinary Journal. Vol. 1. No. 1. 92-107

[21] Rowland, Craig H. (2002). Psionic Software, Inc. Intrusion detection system. U.S. Patent 6,405,318

[22] Lane, Terran D. (2000). Machine learning techniques for the computer security domain of anomaly detection.

[23] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications. Vol. 36. No. 2. 16-24

[24] Linehan, Paul, Shane O'neill, John Donaghy, Armin Lackermeier, and James McKee. (2003). Event queue system. U.S. Patent Application No.10/389,207.

[25] Maindonald, J.H. (1992). Statistical design, analysis, and presentation issues. New Zealand journal of agricultural research. Vol. 35. No. 2. 121-141

[26] Manjeshwar, Arati, and Dharma P. Agrawal. (2001). TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks. In IPDPS. Vol. 1. 189

[27] Rowett, Kevin, and Somsubhra Sikdar. (2005). Intrusion detection system. U.S. Patent Application 11/125,956.

[28] Munger, Edmund Colby, Douglas Charles Schmidt, Robert Dunham Short III, Victor Larson, and Michael Williamson. (2002). Science Applications International Corporation. Agile network protocol for secure communications with assured system availability. U.S. Patent 6,502,135.

[29] Ning, Huansheng, and Hong Liu. (2012). Cyber-physical-social based security architecture for future Internet-of-Things. Advances in Internet-of-Things. Vol. 2 No. 1. 1

[30] Rao, KV Seshagiri, Pavel V. Nikitin, and Sander F. Lam. (2005). Antenna design for UHF RFID tags: A review and a practical application. IEEE Transactions on antennas and propagation. Vol. 53. No.12. 3870-3876.

[31] Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. (2010). The management of security in cloud computing. In 2010 Information Security for South Africa. IEEE. 1-7.