Review of Security Awareness In IOT

L. Selva Packiam [1], D. Radha [2], K. Sivakumar[3], S. Thirumaran[4]
[1, 2, 4] AP, Dept of CSE
[3]AP, Dept of EEE,
[1, 2, 4] Sembodai Rukmani Varatharajan Engineering College, Vedaranyam, Tamil nadu, India
[3]St. Joseph's College of Engineering & Technology, Eluppatty, Tamil nadu, India

Abstract- *The Internet of Things is ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication and wearable computing devices. The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. In this paper, we propose the adoption of a reference ontology to enhance cybersecurity in the IoT considering SA. Anontology extension is used to deal with distinct situational sources and enrich the meaning around security issues.*

Keywords- Security Awareness; Internet of Things; Security Ontology; Cyber Threats

I. INTRODUCTION

Internet of things as the name suggests, is the connectivity of everyday devices with each other. With the advancement in technology, numerous devices are using sensors, actuators, embedded computing and cloud computing. This has enabled communication between devices. To put it simply, the Internet of Things enables devices (things) to interact and co-ordinate with each other thereby reducing human intervention in basic everyday tasks. To get a better understanding of IoT consider the scenario of a smart home.
As soon as the alarm rings it sends a signal to the coffee maker and the toaster, which automatically start doing their jobs without any human intervention.

Thus, saving time and making our everyday tasks easy, this type of device communication is the Internet of Things. The IoT enables physical objects to see, hear, think and perform jobs by having them "speak" together, to share information and to co-ordinate decisions. A network of heterogeneous devices/applications has its own set of challenges. Moreover, as the communication among these devices as well as with related services, is expected to happen anytime, anywhere, it is frequently done in a wireless, autonomic and ad-hoc manner. In addition the services become much more fluid, decentralised and complex.

Consequently, the security barriers in the Internet of Things become much thinner. The IoT architecture, like the Internet, will grow in an evolutionary fashion from a variety of separate contributions, rather than from a grand plan. Security is a major concern while dealing with the Internet of Things. A majority of IoT enabled devices are not very secure and can be accessed by a third party easily. Thus there is a severe need to standardise it to ensure that the privacy of the user is not invaded[1]. Research into the IoT field is still in its early stage, and a standard definition of IoT is not yet available. IoT can be viewed from three perspectives.

1) Internet oriented
2) Things oriented
3) Semantic oriented.

The first definition of Internet of Things was from a "Things oriented" perspective, where RFID tags were considered as things. It was defined as "The worldwide network of interconnected objects uniquely addressable based on standard communication protocols". These definitions do not highlight the industrial view of IoT. Companies across the world are investing billions in the IoT to solve industrial problems (IIoT). The IIoT refers to industrial objects instrumented with sensors, automatically communicating over a network, without any human-to-human or human-to-computer interaction, to exchange information and take intelligent decisions with the support of advanced analytics.

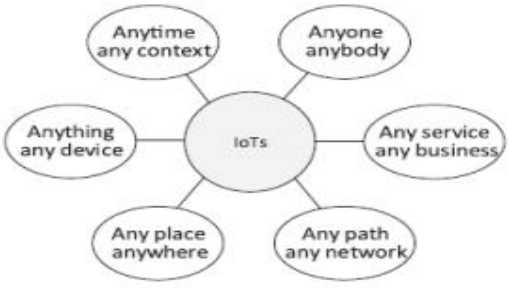

Fig.1. Definition of IoT [3]

The definition of things (as shown in fig.1) in IoT is very wide and includes a variety of physical elements. This network of a variety of objects can bring ample amount of

challenges in developing applications and make existing challenges more difficult to tackle.

II. AN ARCHITECTURAL VIEW OF IOT

A system of large-scale and heterogeneous IoT end devices can be used to collect large volume of data. Analysis of the collected data facilitates the building of an intelligent world [3]. While intelligence may be the goal of IoT, data is the key to achieve that goal. Illustrated in Fig 1 is a typical three-layer IoT architecture. IoT applications run on top of a stack of three layers, including the Cloud layer, the Edge layer, and the Things layer. Each layer is capable of collecting, processing, and analyzing data. Although data is mostly streamed from the things layer to the cloud layer through the edge layer, the other direction of data flow is also supported in applications that send commands to the end devices in order to control the physical world.

The things layer consists of a large scale of heterogeneous end devices (sensors and actuators). These devices are tightly coupled with the physical world; such tight coupling enables the devices to closely monitor the physical world. The heterogeneous end devices may have significantly different capabilities in terms of computation, storage, communication, and power supply. For example, some devices like smart meters are powerful enough to satisfy reasonable heavy computation requirements, while others like RFID tags can only store several bytes of information and barely have any computation capability. There are also actuators in this layer to execute commands sent by the IoT applications.

Generally speaking, most devices in this layer are resource-constrained and energy-limited. Therefore, those devices are not able to perform heavy tasks. Mining intelligence from the data requires a cluster of computational and storage resources working together to process huge volume of data. Therefore, the cloud layer is suitable for this purpose in that it has sufficient storage space and computation power, and almost unlimited power supply. Moreover, many powerful tools and advanced algorithms are ready to be utilized in the cloud. On the other hand, the cloud is usually located far away from the end devices and cannot directly communicate with the end devices. The cost of migrating the data processing to the cloud may be prohibitive.

In addition, this approach does not support applications where high real-time requirements, extensive geo-distribution or high mobility are desired [2]. To fill the gap between the low capable end device layer and the powerful but faraway cloud layer, the edge layer (also called the fog layer or the gateway) is added to the architecture. Edge devices are located physically close to the end devices and are generally much more powerful than the end devices. Edge devices can not only mask the heterogeneity of the end devices by providing multiple communication interfaces, but also offload the overhead of data processing and analyzing from the end devices. Moreover, with high speed network connection, it is much easier for the edge devices to get help from the cloud layer when necessary, or they can work together with the cloud layer to complete the tasks. It is in this sense that we consider the edge layer plays a critical intermediary role in this architecture.

Fig 2. An Architectural View Of IOT

In summary, in order to create a connected, intelligent environment, it is essential to make these three layers work together efficiently in an IoT system; tasks of the IoT systems need to be deployed in the appropriate layer based on the requirements of the tasks.

III. THREATS IN IOT SYSTEM MODEL

A generic IoT system can be fully represented and describedby using three main key layers: Perception, Transportation and Application. In fact, in [4] the security problems of each layer are analyzed separately by looking for new robust and feasible solutions.

A. Perception Layer

The first layer is related to the physical IoT sensors to support data collection and processing on different common technologies such as RFID (Radio-Frequency IDentification), WSN (Wireless Sensor Network), RSN (RFID Sensor Net-

work) and GPS. This layer includes sensors and actuators to perform different measurements (i.e., temperature, acceleration, humidity, etc.) and functionalities such as querying location [5]. Due to the limited node resources and distributed organized structure, the main security threats coming from the Perception layer are the following:

- Physical Attacks: These kinds of attacks are focused on the hardware components of the IoT system and the attacker needs to be physically close or into the IoT system in order to make the attacks working. Some examples of these attacks are:
    - Node Tampering: The attacker can cause damage to a sensor node, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information, such as shared cryptographic keys or routing tables.
    - Malicious code Injection : The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system.
- Impersonation: authentication in the distributed environment is very difficult, allowing malicious nodes to use a fake identity for malicious or collusion attacks
- Denial of Service (DoS) Attacks: attackers exploit the finite processing ability of the nodes, making them un-available.
- Routing Attacks: intermediate malicious nodes (e.g. in a WSN) might modify the right routing paths during the data collection and forwarding process.
- Data Transit Attacks: various attacks on the confidentiality and integrity during data transit (e.g. Sniffing, Man-In-The-Middle).

B. Transportation Layer

Transportation layer mainly provides ubiquitous access environment for the perception layer. The purpose of this layer is to transmit the gathered information, received from the perception layer, to any particular information processing system through existing communication networks used by both Access Networks (3G, WiFi, Ad hoc network, etc.) or Core Networks (Internet).

TABLE I THREATS IN IOT SYSTEM MODEL

Layer	Main threats
Application Level	Data Leakage
	DoS Attacks
	Malicious Code Injection
Transportation Level	Routing Attacks
	DoS Attacks
	Data Transit Attacks
Perception Level	Physical Attacks
	Impersonation
	DoS Attacks
	Routing Attacks (e.g. in WSN, RSN)
	Data Transit Attacks (in WSN or RSN)

In [6] there is a brief overview of security issues in wireless networks such as cellular networks. According to this study, the open and heterogeneous architecture of an IP-based LTE network, is resulting in increasing number of security threats compared to the 3G networks. Generally, at this level, the main security threats are:

- Routing Attacks: intermediate malicious nodes (e.g. in a WSN) might modify the right routing paths during the data collection and forwarding process.
- DoS Attacks: because of the heterogeneity and complexity of IoT network, the Transportation layer is vulnerable to get attacked.
- Data Transit Attacks: various attacks on the confidentiality and integrity during data transit in access or core networks.

C. Application Layer

The application layer provides the services requested by customers. For instance, the application layer can provide temperature and air humidity measurements to the customers asking for such data. The importance of this layer for the IoT is that it has the ability to provide high-quality smart services to meet customers' needs. Many different IoT environments (i.e. smart city, smart healthcare, smart factory) can be implemented within this level; moreover, an Application Support Sub-layer (ASS), to support all sorts of business services and to realize intelligent computation and resources allocation, could be implemented throughout specific middleware and cloud computing platforms.

The main security threats within this layer are:

- Data leakage: the attacker can easily steal data (also data user e.g. user password) by knowing vulnerabilities of the service or application.
- DoS attack: attackers can destroy the availability of the application or service itself.
- Malicious code Injection: attackers can upload malicious codes in software applications exploiting the known vulnerabilities.

IV. ONTOLOGY-BASED SECURITY AWARENESS TO ENHANCE SECURITY IN THE INTERNET OF THINGS

In this section, we present an ontology-based approach to enhance the security in the Internet of Things using a security awareness paradigm, which explores data collection to building the knowledge about the reality of the IoT environment. There are many languages proposed in the literature to development for semantic computing. Among them, the ontology-based modeling technique is a suitable logical language for modeling dynamic context and situation [7, 8]. In the case of security awareness, this technique has advantages to the representational aspects and, mainly, to the reasoning issues as well as making inferences of others facts using the reasoning engine using inference rules [9,10].

Sensors collect attributes of IoT security in the environment, and once a situation is identified and classified, the neighborhood is communicated to understand the potential characteristic of the situation. In many cases, it will avoid communications and data exchange with compromised sensors. In the following sections, we describe the scope of categories of situations of interest addressed in this paper. Each category has a set of rules that apply a situation considering particular aspects of these types of situation. To identify each category in the knowledge base of the IoTSec ontology, we use the SPARQL language 1 to express semantic queries [11].

A. Situation Specification for a IoT Security Ontology An approach using security awareness to enhance the security in the Internet of Things considers a building of knowledge from collected data of sensors. In this context, information about authentication tools, IDS alerts, firewall diagnostics exceptions, access localization, number access attempts, and so on. All this information is developing knowledge aboutreality and in this paper uses a formal representation through ontologies to manage the whole system, instances and their relationships. For example, port scanning from specific IP addresses attached with some access attempts in multiple ports. Moreover, some firewalls exceptions from the same IP address.

These pieces of information from different sources can be combined to identify attempts in infiltrating a system using
multiple channels. We specify an extension to the IoTSec ontology to build the knowledge about the reality. This ontology extension is generic to represent all situation facts and associate to classes of the IoTSec ontology. Each situation fact should be associated witha particular class cited in the Section V following their security attributes. We take in consideration which kind of device generated each alert and use all attributes to be analyzed and aggregated with others situations facts.

For example, a vulnerability of the unprotected communication channel generated from a source vulnerability scanner in a specific device should be associated with the vulnerability class. After few minutes, an IDS source detected an attempt of the sniffer activity the same communication channel. Therefore, the IoTSec ontology has capability to make inferences based on these two situation facts and suggests that there is a situation of the interest involving an unprotected communication channel and this could be protected by using a criptography scheme. In this case, situation facts are identified from security tools, but they can be generated from situational sources with malicious activities associated with cyberthreats. In these cases, a collection of security metrics are built to use in the inferences of the ontology.

B. Inferences

In this work, we adopt the Semantic Web Rule Language(SWRL) 2 to define rules inference rules to be processed by the inference engine. An example where we could use a rule refers to a situation where a security mechanism, a threat, and security properties are mapped in the ontology. We know that when a threat occurs, this will affect one or more security properties. In this case, if a security mechanism protects this threat, consequently, this security mechanisms satisfies the same security properties.

SecurityMechanism(?sm) ˆ Threat (?t) ˆ
SecurityProperty(?sp) ˆ affects(?t, ?sp) ˆ
isSecurityMechanismOf(?sm, ?t)
→ satisfies(?sm, ?sp)

When the system process this rule, the engine can infer that the security mechanism protects a threat that affects some security properties, we also can say this

security mechanism satisfies these security properties.

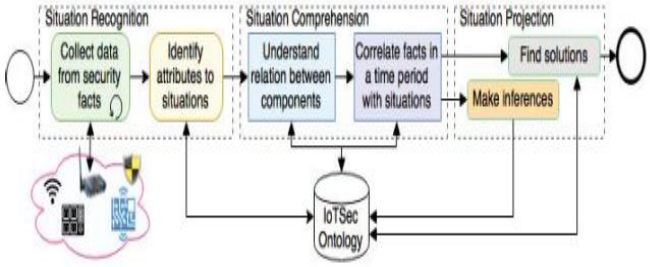

Fig. 3. Workflow to analysis of situation of interest from IoT environment.

This new fact will be useful when queries were done looking for which do security mechanisms protect one specific security property. As this is not explicit, the outcome of this inference rule will result in enrichment to the cyber security.

An authentication system is used to identify and authorize only known users in the network. Moreover, sensors can detect unauthorized users trying to take access to read or destroy transmitted data. The simple data analysis of these security alerts is only looking for automated alerts generated by intrusion detection systems based on signatures. On the other side, more advanced correlations can prevent one of the security issues aforementioned as well as user's location with access to private information.

V. CONCLUSION

IoT is the process of automation of all the devices. It is being used in most of the daily life matters like medical, customer services, marketing, auto industry, retail outlets by using different sensors. The two basic technologies of IoT can integrated with each other for better interoperability.

Although this proposal is on conceptual level, this paper proposed the use of ontologies to building knowledge about the reality of the IoT environment. This knowledge can be using simple automated alerts generated from distributes sources like

IDS, firewalls exceptions, or using the advanced correlations between access attempts, network probes with time and loca-
tion data.

Thus, it is crucial, in the next future, to start working on the the critical issues of this level implementing lightweight security solutions that can adapt to the heterogeneous environments with resource-constrained devices.

REFERENCES

[1] Ala Al-Fuqaha , Mohsen Guizani , Mehdi Mohammadi "Internet of things: a survey and enabling technologies, protocols and application" IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, Fourth Quarter 2015.

[2] F. Bonomi et al., Fog computing: A platform for internet of things and analytics. Springer International Publishing, 2014.

[3] J. Gubbi et al., "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol.20, no. 8, pp. 2481-2501, Nov. 2014.

[5] K. Lin, M. Chen, J. Deng, M. M. Hassan, and G. Fortino, "Enhanced Fingerprinting and Trajectory Prediction for IoT Localization in Smart Buildings," in IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1294-1307, July 2016.

[6] S. Barakovi et al., "Security issues in wireless networks: An overview," in Proc. XI International Symposium on Telecommunications (BIHTEL), Sarajevo, 2016, pp. 1-6.

[7] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni, "A survey of context modelling and reasoning techniques," Pervasive and Mobile Computing, vol. 6, no. 2, pp. 161–180, 2010.

[8] D. Riboni and C. Bettini, "Owl 2 modeling and reasoning with complex human activities," Pervasive and Mobile Computing, vol. 7, no. 3, pp. 379–395, 2011.

[9] M. M. Kokar and M. R. Endsley, "Situation awareness and cognitive modeling," IEEE Intelligent Systems, vol. 27, no. 3, pp. 91–96, 2012.

[10] S. S. Yau and D. Huang, "Development of situation-aware applications in services and cloud computing environments," International Journal of Software and Informatics, vol. 7, no. 1, pp. 21–39, 2013.

[11] B. A. Mozzaquatro, R. Melo, C. Agostinho, and R. Jardim-Goncalves, "An Ontology-based Security Framework for Decision-making in Industrial Systems," in Model-Driven Enterprise Services and Applications for a Sustainable Interoperability: New Paradigms for Development in the Future Enterprise - MDE4SI, 2016, pp. 779–788.