JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
31st December 2017, Volume 2, Issue 3, JSEIS, CAOMEI Copyright © 2016-2017
www.jseis.org

A new centralized-distributed layers model to enhance the security of IoT

[1] Hazem M. Bani-Abdoh, [2] Fuad M. Fatfath
UniSZA University, Malaysia
Email: hazem.ersan@gmail.com, fuad.fataftah@gmail.com

ABSTRACT

Internet of Things (IoT) is an emerging technology that penetrates into every aspect of human being. IoT is a network of connected IP devices. Since, IoT is mainly encompassed networking of IP devices, it emerges concept of sharing, thus, it must encounter challenges to privacy and security/threats. IoT covers different devices, these devices are governed with different technologies. These diverse technologies are associated with security or securing IoT networks. This research investigates the concept of IoT, its challenges, and the privacy and security issues. In addition, this research proposes a new centralized-distributed layers model (SIAM) to enhance the security of IoT. This model manages all of the collaboration's and heterogeneity's concerns. In reality, SIAM is able to represent different rules included in different types of independent organizations. It is also able to express the security policies for centralized and distributed structures as in IoT scenarios. SIAM includes the core concepts of the context and collaboration.

Keywords: internet of things; IoT; security model; privacy; security; IP devices;

1. INTRODUCTION

Internet of Things (IoT) is the network that is developed from a huge network connecting billions of wireless identifiable devices, objects and physical devices, interacting with each other with anything, anytime, anywhere [1]. In the field of management of information, the achievement of goals can formulate an influence on organizational performance, financial lack or organization's credibility without consideration to risk. IS is the name for the risk control of the negative influences and utilization of possibility in accomplishing enterprise aims and intentions [2]. Availability, integrity and authenticity of information must be maintained as information is considered one of the major components within an organization, and national security [3]. Organization with a strategic and IS threats contains security information to become a primary part of it. However, the more information that is controlled and ran by the organization, the larger is the risk of threats to the information.

Confidentiality, integrity and availability of information have dimensions of IS as a part of its setting and context which means dimensions of IS are continually in the setting of the accomplishment for objectives of business or organization missions. The leaking of information, waste of information or insufficiency of information is blocked and interrupted by the usage of IS risk control. IS turned to be a highly significant part to be employed in the organization by these conditions [2]. On the other hand, security awareness is considered another fundamental part that hugely influences the security of information [4]. This research article aims to investigate the security and privacy of protocols used in IoT; providing a comprehensive analysis of current solutions in the IoT's privacy/security concerns; discusses different solutions to basic concepts of security; provides solutions to the problems troubling the IoT; and designs a secure platform of IoT architecture. The proposed model, in reality, is able to represent different rules included in different types of independent organizations. It is also able to express the security policies for centralized and distributed structures as in IoT scenarios.

2. IS GOVERNANCE

Information technology (IT) is considered as an extremely primary entity in the regular activities of an organization, due to this it is a priority for the IT infrastructure to be administered and ruled accurately. Ensuring the value of well IT governance comes from the institute of directors' report [5] on corporate governance. IT highlights that resource utilization, goals/services delivery, and risk management must be concentrated by its governance. From the viewpoint of the IT governance institute [5], the main components of the IT governance are the administration, organizational structures and processes. The main role for the mentioned components is to ensure that the organization's IT preserves and enlarges the organization's strategies and objectives. Moreover, to guarantee that the organization's IT supports the business objectives, maximizes profits and possibilities, and aids in obtaining competitive advantage, its governance should result in a combination of good practices [5].

One of the main aspects of the information security (IS) governance is that it should serve valid IS practices by following a precise direction and should produce and present organizations with a recognition of the necessary aspects for a comprehensive IS plan. The organization's needs and risk appetite also must be reflected by this IS plan [6]. Figure 1 shows that the strategic level is where the directing should begin at, and proceed through the tactical level and ended up with the operational level. The executive level directions in the direct process, are distributed and cascaded in the IS policies into lower-level. To assist in reaching to the tactical level and consequently to the strategic level controlling catching the operational data from the lowest execution layer.

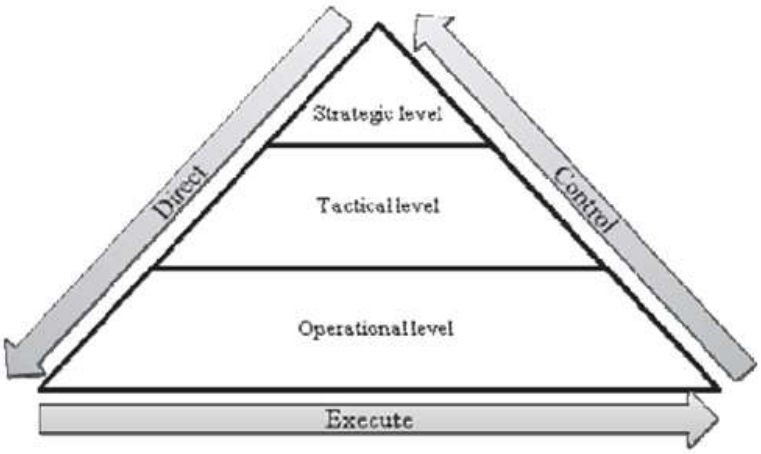

Figure. 1 Information governance model [6]

IT probably tracks executive management directives from the strategic level if IS governance applications are implemented efficiently, that can be done through the tactical level, onto the operational level. Moreover, control checking that occurs with the operational data is obtained at the lowest execution layer, within the operational level, the tactical level, to the strategic level. it can be argued that organization can actually claim agreement to IS governance only when directing and controlling are performed at all management levels [7].

3. INFORMATION SECURITY RISK MANAGEMENT

In the IS program management, risk management is considered as a significant portion that is arising from the organizational risk governance [7]. The definition for the term information risk management can be said as the "process of recognizing risk, evaluating the reasonableness of its happening and the influence it possibly holds and considering the action required to assure that the compensation from the activities presented will be received" [7]. The definition for IS program management distinguished the following main elements of risk management: (a) identification of risks (b) assessment of risks (c) actions to mitigate the risks (d) determining whether the reward is worth the effort, and (e) resources engaged to mitigate the risks. Consequently, in [8] the research outlined the elements of risk management to four blocks essential for recognition and handling IT risks, specifically discovery, measurement, classification, and prioritization.

In the organization managing risk exists to preserve and defend the mission and assets of the organization. That is why risk management must not be a technical function and be a management function. It is essential to manage risks to systems. The owner of any system can protect the information system in the organization by understanding risk, understanding the precise risks' effects to the system. Organizations can never be decreased to zero due to the fact that they all have limited resources and risk. Therefore, allows organizations to prioritize limited resources by understanding risk, mainly the quantity of the risk. Identifying threats and vulnerabilities gives the ability to assess the risk, then recognizing the probability and consequence for every risk. It's clear, right?, risk assessment is a complex undertaking which something unfortunate, normally based on defective information. Thus, many methodologies pointed at supporting risk assessment to be repeatable and give consistent results [7]. Financial institutions and insurance companies employed quantitative risk assessment based upon methodologies. By attaching conditions and values to business processes, information, systems, recovery costs, etc. Accordingly, risk can be estimated in terms of direct and indirect costs.

A large range of uncertainty in the likelihood and impact values and describe them are assumed by qualitative risk assessments, and also risk, in subjective or qualitative terms. Comparable to the subjects in quantitative risk assessment, the likelihood and impact values are being defined by the numerous difficulties in qualitative risk assessment. Moreover, to allow the similar rules and scales to be consistently applied across varied risk assessments and these values need to be determined in a manner that can do this [8].

The outcomes of qualitative risk assessments are naturally more complex to concisely communicate to management. Results of "high", "moderate" and "low" risk are degrees which typically given by qualitative risk assessments. Yet, it is potential to appropriately communicate the assessment to the organization's management by implementing the impact and likelihood definition schedules and the classification of the Impact.

Steps [7-9]:

1. Identifying threat

   Both threat-sources and threats need to be recognized as was alluded to in the part on threats. Threats should incorporate the threat-source to assure correct assessment. (Natural threats, human threats, deliberate actions, environmental threats).

2. Identifying vulnerabilities

   Vulnerabilities come with many ways of identifications. Several risk management plans give many methodologies for recognizing vulnerabilities. Begin with ordinarily available vulnerability tables or control states in a general way. Later, running with individuals or the system owners with knowledge of the system or organization, begin to identify the vulnerabilities that apply to the system. Additionally, while the following tools and techniques are typically used to identify vulnerabilities:

- ✓ Vulnerability scanners
- ✓ Audit of operational controls; and
- ✓ Penetration testing.

3. Relating threats to vulnerabilities

   Relating a threat to a vulnerability is considered one of the major complex activities in the risk management process. Anyway, it is a mandatory activity to establishing these relationships, since risk is determined as the instance of a threat against a vulnerability.

4. Defining likelihood

   It is fairly straightforward when determining likelihood. It is the possibility that a threat produced by a threat-source will happen versus a vulnerability. It is an outstanding concept to employ an official definition of likelihood on all risk assessments in order to assure that risk assessments are consistent.

5. Defining impact

   The best way to define impact is in terms of impact upon availability, impact upon integrity and impact upon confidentiality in order to assure repeatability.

6. Assessing risk

   The process of deciding the likelihood of the threat being applied against the vulnerability and the resulting influence from a successful compromise is called the process of assessing risk. When assessing likelihood and impact, take the current threat environment and controls into consideration. For each risk in the risk assessment report, a risk management strategy must be devised that reduces the risk to an acceptable level for an acceptable cost. Steps [9].

- Transference
- Mitigation
- Avoidance
- Acceptance

- Communicating risks strategies
- Implementing the strategies

4. INTERNET OF THINGS – IOT

This section is organized as follows: An introductory to the IoT, need for the IoT and security issues of the IoT. This section provides a brief introduction of IoT, the need for IoT in the organizations, data management in IoT, IoT challenges, challenges protocols that are used in IoT.

4.1 Introduction

The sight of IoT is mainly to revolutionize the network (Internet) by building a huge network connecting billions of wireless identifiable devices objects and physical devices, interacting with each other with anything, anytime, anywhere. The existing improved processing, and storage capacities and wide distribution capabilities of wireless sensor networks (WSNs), RFID technologies may create a highly shared-decentralized pool of available resources and devices interconnected with each other [1]. For the time being, around two billion users around browse the Internet, using social networks, playing games, accessing multimedia, sending and receiving emails, and many other available tasks. With more access to the resources, available information and infrastructure, another important hop is coming, which is the use of the network as a global and shared platform for allowing devices and smart physical objects dialogue, compute, communicate, and coordinate. The IoT term refers to [10].

- The common network connecting smart-physical objects;
- The group of technologies necessary in order to realize such a IoT vision (such as: actuators, RFIDs, etc.); and
- The set of services enhancing such technologies in order to create strong new market opportunities [10].

4.2 Need for IoT and organizations of interest

In the past, accessing the internet has dramatically done by using desktop or laptop devices, nut nowadays it is evolved to use mobile devices like: Televisions, IPads, Mobiles, etc. In this field a new emerging technology called IoT (IoT) is quickly taking a place. The main base of this paradigm is to make each physical object as a part of Internet, communication with each other's in order to reach a shared goal (i.e. the IoT attempts to link (connect) the physical objects found in its environments to the digital one's). Figure 2 shows the paradigm of IoT [11].

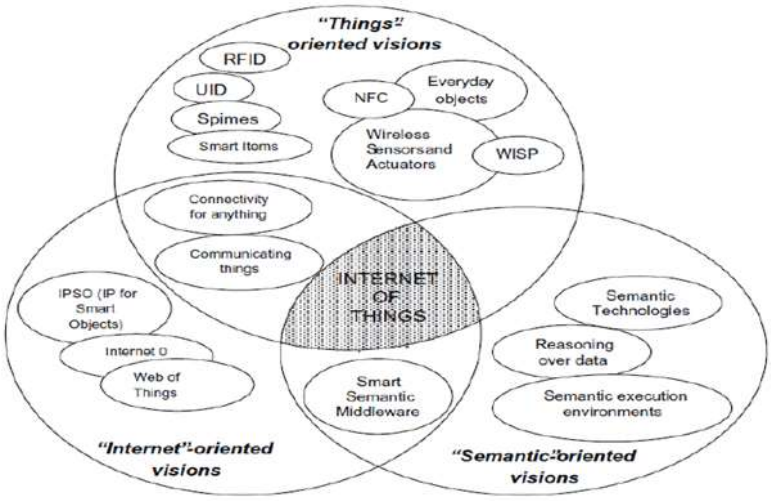

Figure. 2 Internet of things paradigm. [11]

Unlikely, IoT rises as a brand of new technologies. An incremental and progressively development, along with IoT current technologies will be effectively used in order to extend and enhance current ICT applications, offering a lot of additional features, attributes and capabilities related to the ability of communicating with the physical world. As shown in Figure 3 below, IoT consists of different technologies involved or (will be involved) in the future of IoT environment [11].

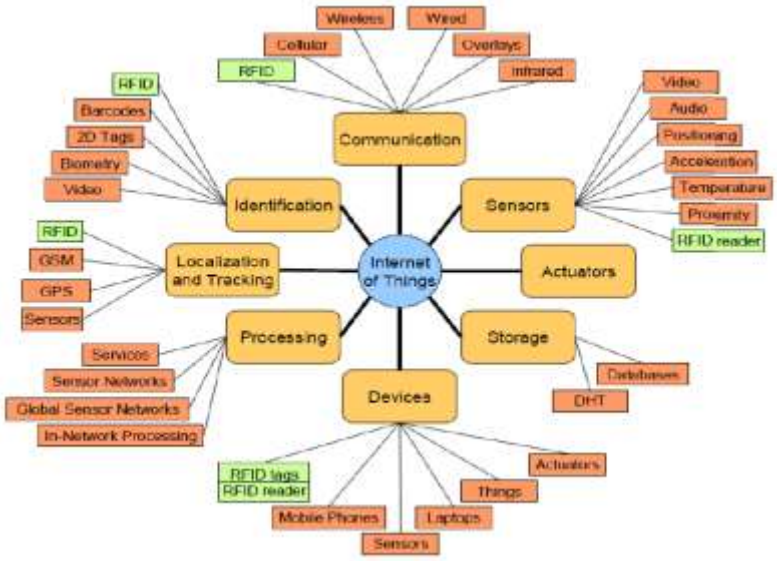

Figure. 3 The main elements of IoT [11]

4.3 IoT data management

Data management systems (DMS) manage the storage, retrieval, plus renew of elementary information items, files and records. In the setting of IoT, (DMS) need to review and summarize data online at the same time enable logging, providing storage, and auditing facilities for offline examination. This extends the idea of data control from query processing, offline storage and transaction management operations into online-offline communication/storage dual operations.

a) Data lifecycle

The lifecycle of data in an IoT system (Figure 4) continue from data generation to collection, transfer, voluntary filtering, and state of preprocessing, and lastly to archiving and storage. Querying and analysis are the last result that launch (request) and use data production, but be pushing it to the (IoT) consuming services. Collection, filtering, Production, aggregation and some fundamental querying and preparatory processing functionalities are considered online, communication-intensive operations. Concentrated preprocessing, storage with long-term and archival and in-depth processing/analysis are considered offline storage-intensive operations [12].

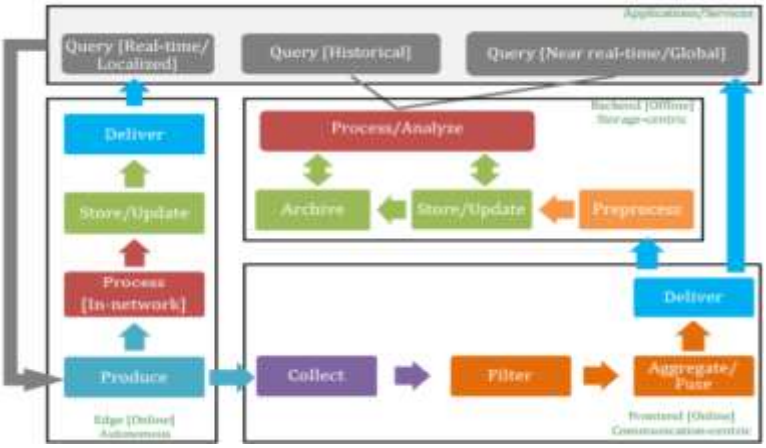

Figure. 4 Data management in IoT [12]

Making data open and accessible in the long term for regular access/updates, at the same time archival is involved with read-only data is the aim for Storage operations. Without any need to generate data further up to concentration points in the system some IoT systems can produce, process, and store data in-network for real-time and localized services [5]. In the next paragraphs, every element in the IoT data lifecycle is described:

- *Querying*: In the setting of IoT, a query can be assigned either to ask for a real-time data to be gathered for temporary monitoring aims or to recover a particular view of the data stored in the system.
- *Production*: It includes understanding and transfer of data by the Things in the IoT framework and summarizing and reporting this data to involved participants regularly, driving it up the network to aggregation points and afterward to database servers, or expressing it as a response triggered by inquiries that ask the data from sensors and smart objects.
- *Collection*: The sensors in the IoT can store the data for a specific time or report it to directing parts. Data can be gathered at assembly points or gateways in the network where it is extra filtered and treated, and maybe combined into compact structures for efficient transmission.
- *Aggregation/Fusion:* all the new data out of the network that Transmitting in real time is frequently growing data flowing rates and the restricted bandwidth. Gathering techniques use summarization and merging processes in real-time to decrease the volume of data to be stored and transferred.
- *Delivery*: While data is aggregated, separated, clarified, filtered and probably processed either at the assembly points or at the independent virtual part within the IoT, the outcomes of these processes will require being posted further up the system, either as concluding answers, or for storage and in-depth analysis.
- *Preprocessing*: IoT data will arrive from many origins with differing compositions and formations. It may require being preprocessed to manage lost data, eliminate repetitions and combine data from various origins into a united schema before being assigned to storage.
- *Storage/Archiving*: This state controls the effective storage and preparation of data, as well as the constant, renew of data with new information as it shifts to be available. Archiving relates to the off-line long storage of data that is not directly required for the system's continuous operations.
- *Processing/Analysis:* This state requires the continuous retrieval and review operations executed and collected and archived data in order to obtain penetrations into past data and predict future aims, or to identify irregularities in the data that may trigger additional inquiry or performance.

4.4 IoT challenges

IoT as a service needs some kinds of requirements, such as:

- *Interoperability*: With respect to different organization polices, the organization can use its own policy. So, IoT should be effectively modeled in order to support different types of organizations.
- Context awareness: Context is very important in the environment of IoT [13, 14]. As, the applications employ knowledge from the context to gain information about users' environment [15-17].
- *Ergonomic:* Non-expert consumer may use the services, so the used mechanism in access control must be simple as much as possible to use.
- *Heterogeneity*: An IoT environment is considered as a collaborative environment, because it contains different [18-21]. This heterogeneity feature may result in complicated interoperation issues, such as different vendors provide completely different devices, which offering different features able to be accessed by several services using different behaviors and protocols [22].
- *Lightweight solution*: The mechanism of access control may reduce the usage of resources because of the nature of the IoT devices that characterized by its constrained energy.
- *Scalability*: Managing vast volumes of devices, users, and applications must be done in a scalable manner. Furthermore, the mechanism of IoT must naturally be characterized by its extensibility in different number of organizations, structure [20].

A lot of challenges may affect the development of IoT due to two main reasons: connection between objects (devices), and numerous collecting of information for each object included in the IoT system. These challenges are [23, 24]:

1. Standards challenge and interoperability problem

In fact, standards are very critical everywhere we develop any new technology. There is a relation between interoperability and standards, while the interoperability will be more complex when different devices (objects) from different providers do not employ the same standards, thus why it new another additional gateways in order to translate different standards.

2. Radio spectrum challenge

The expected huge growth in the volume of used wireless devices in IoT needs a huge radio spectrum. Based on the extent of using different technologies such as Wi-Fi and Mobile-Wireless, the type of using spectrum must be allocated in the IoT.

3. Security issues

The development of IoT brings additional of security challenges to users, to organizations, and to business. Capturing sensitive, data unauthorized access, attacking servers, and intercepting network communications may be types of the security issues in IoT.

4. Privacy issues

Privacy issues concerns with the protection of user's privacy. As the information must be privately transmitted to the endpoint.

5. Data Understanding challenge

Analyzing the gathered data is being successful depending on the correctness degree of preprocessing of data. While the preprocessing is mainly depending on the ranges of characteristics of observations which is estimated from data itself.

6. Standardization challenge.

Standardized protocols is required in order to query Meta- information by devices and sensors. As well as it may be required to exchange of raw data.

7. Complexity, and integration issues.

Testing and integrating IoT systems with different platforms, protocols and APIs, will be a challenge. The quick development of APIs consumes unexpected resources that will significantly reduce the ability to extend the system by adding new features or new core functionalities.

8. Evolving architectures challenges.

With so many players, users, and technologies involved with the IoT system, it is bound to be continuous wars between legacy providers in order to hold strong systems advantages, features, and suitable competitive advantage. Figure 5 summarizes the possible challenges and risks faced by IoT layers. The possible threats to the Perceptual Layer of IoT are [25]:

- Node damage
- Information tampering
- Forgery attacks
- Replay attacks
- Fake attacks
- Channel blocking; and
- Copy attacks and so on.

While the challenges, that may affect the Transport Layer, are:

- Heterogeneous network attacks
- DOS attacks
- Counterfeiting attacks

- Network security threats
- Application risks
- Conflicts of WLAN application and so on.

As the threats of the Application Layer are:

- Unstable platform
- The information disclosure
- Authentication and
- Illegal human intervention.

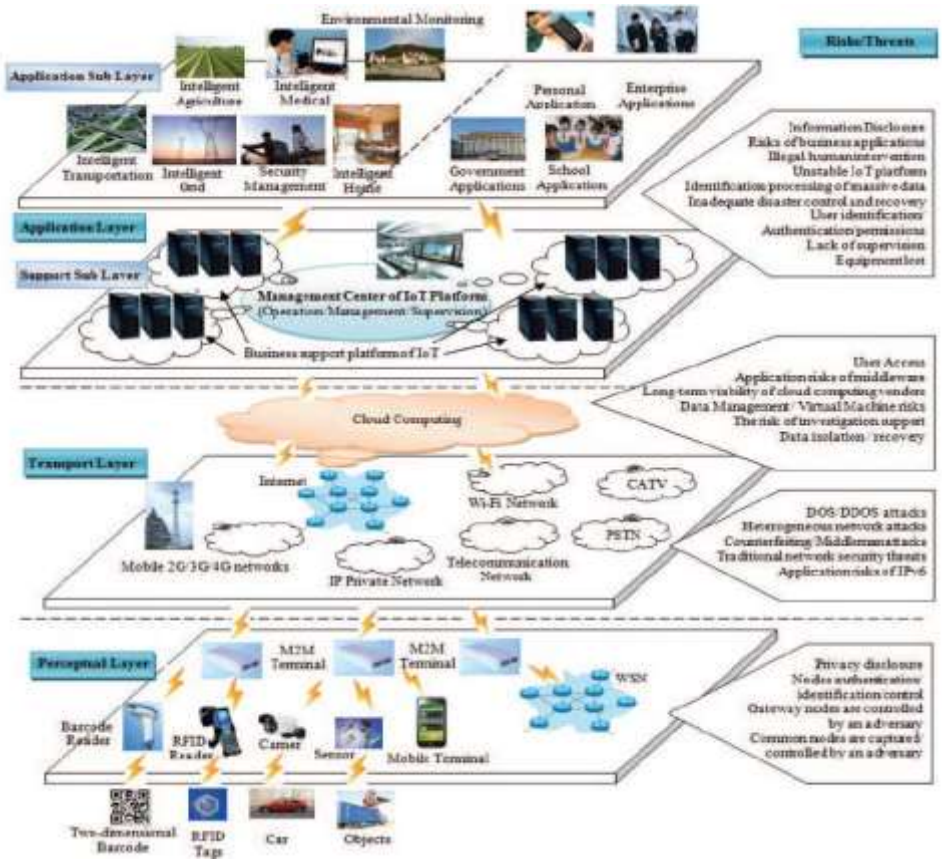

Figure. 5 Security challenges of IoT [25]

4.5 IoT security protocols

It is obvious that Security is another feature of IoT applications which are significant and can be detected nearly in all layers of the IoT protocols [26]. All layers contain Threats incorporating application layers, data link, session, and network. In this part, we shortly review the security tools created in the IoT protocols [27].

4.5.1 MAC 802.15.4

It grants several security methods in the Frame Control field in the header by employing the Security Enabled Bit. Security requirements include secured Time-Synchronized Communications, confidentiality, integrity, authentication, and access control mechanisms.

4.5.2 6Lo WPAN

The 6Lo WPAN itself gives no proposition to mechanisms for security. Besides, related reports involve investigation of security threats, demand and procedure to take into consideration in IoT network layer. For instance,

RFC 4944 addresses the opportunity of duplicate (EUI-64) interface addresses that are thought to be uncommon (RFC4944). RFC 6282 addresses the security concerns that are constructed due to the obstacles presented in RFC 4944 (RFC6282). RFC 6568 discusses potential tools to select security within restrained wireless sensor mechanisms [RFC6568]. Moreover, a few up-to-date designs in [6Lo] review mechanisms to complete security in 6loWPAN [27].

4.5.3 RPL

By employing a (Security) field subsequent the 4-byte ICMPv6 message header the RPL contributes a distinct level of security. Data in this field shows the cryptography algorithm and the security level employed to encrypt the message. RPL offers protection versus replay attacks, assistance for information authenticity, confidentiality key management, and semantic security. Levels of security in RPL include Authenticated, Preinstalled, and Unsecured. RPL attacks involve Hello Flooding, Particular Forwarding, Sybil, and Sinkhole, Denial of Service attacks, Black hole and Wormhole.

4.5.4 Application layer

Applications may afford an extra level of security utilizing TLS or SSL as a carrier layer protocol. In addition, to handle various levels of security as needed, an end to end authentication and encryption algorithms can be employed.

5. SECURE IOT ACCESS MODEL (SIAM)

Secure IoT Access Model (SIAM) introduces the main concept of any institution as a collection of structured active entities interacted with each other. The entity's activity is defined as a set of actions, but the entity's view is defined as a set of objects, as well as the entity's context is defined as specific situation. The entity's role actually establishes structure of the connection link the Subjects and the organization itself. The relationship (org, r, and s) indicates that organization (org) utilizes specific subject (s) in specific role (r). Similarly, any objects which commonly satisfy a property can be directly specified using the action's activities and views.

Based on the security rules, we can be similarly defined the Prohibitions, Obligations, and Permission as (org, r, v, a, c). While (c) indicates the context, (org) indicates organization, (r) is the organization's role (r), (a) is the organization's activity, and (v) indicates organization's view. Each (r) can be expressed through an entity, SIAM specifies the security policies of the heterogeneous organizations. Furthermore, SIAM takes into account the organization's context like (the constraints of locations as well as the time).

In addition, SIAM is comprehensively adapted to the IoT technology. As it can manage all of the collaboration's and heterogeneity's concerns. In reality, SIAM is able to represent different rules included in different types of independent organizations. As it is also able to express the security policies for centralized and distributed structures as in IoT scenarios. SIAM includes the core concepts of the context and collaboration.

5.1 SIAM Architecture

Different architectures can be used to access control such as:

- Centralized architecture

This architecture has a single entity (called central entity) that perform the authorization process, On the other hand, sensors and actuators don't play a significant role in this architecture, as the control process is fully located within a central entity).

- Distributed approach

In this approach, the access control for any resource is not actually located in centric device, but it is located in all of the end devices in IoT. As result, this approach allow the end-devices to act independently, effectively and smartly.

- Centralized-distributed approach

This approach gives the end-devices more intention by allowing them to partially participate in the process to convey the possible delays that may occurs when transmitting the information to the central entity.

In our proposed model, we used *Centralized-distributed Approach. We suggest to provide* central authorization device in each separate set of IoT components. The selection of the entity that must perform the authorization process

at specific time mainly depends on the contextual feature in that set's node as shown below in Figure 6. Thus, the process will performed in efficient time and smoother information exchange between the authorization engine and end devices. Absolutely, not all of the available devices have the same degree of constraint in the IoT environment.

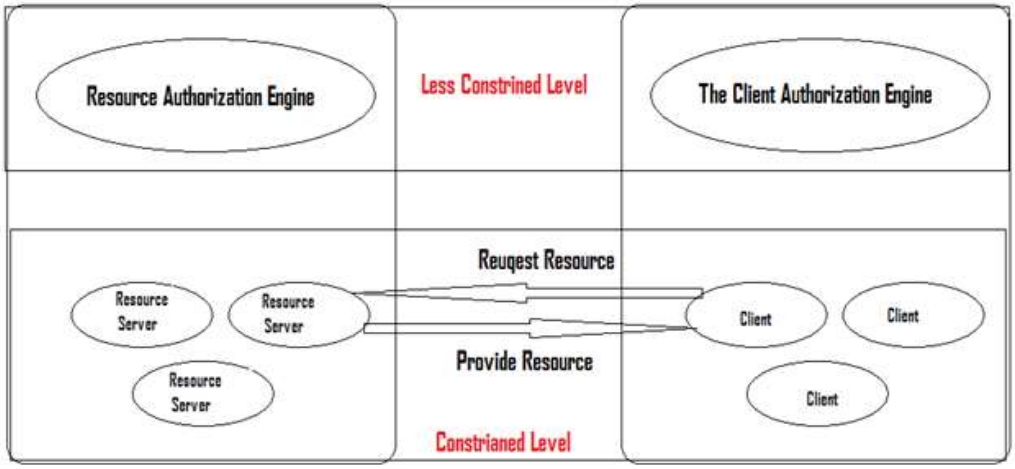

Figure. 6 Centralized-distributed layers

The main components of our model are:

- Client Owner (CO)

CO component owns the whole Client as well as it controls all of related authorization permissions of a Resource (R);

- Resource Server (RS)

CO component hosts a Resource (R), (R) can holds information or values, sensor or actuator;

- Client (C)

(C) is the component which asks to access a (R) from (RS);

- Resource Owner (RO)

(RO) is the entity that holds the resource and its access permissions;

5.2 SIAM Layers

The SIAM model is proposed based on dividing the authentication process into four main layers as shown in Figure 7 Each layer has different capabilities, since each device is located to a different layer. These layers are:

- Less Constrained Layer

In order to mitigate the nodes that perform complex tasks in of constrained layer, this layer is used. Every set of actors in the constrained layer is associated to specific actor of this layer based on specific security domain. The component of the client part is called "Client Authorization Device" (CAD), and the component of the provider part is Resource Authorization Device (RAD).

The *CAD and C* have the same security structure. It allows *C* to decide if *RS* is an unauthorized source or not for *R* by gaining required information for the authorization process, as it helps *C* to control the authorization process. On the other hand, the *RAD, R, and RS* have the same security structure. It helps RS to get the permission of *C* to access the resource R. Moreover, *RAE* helps *RS* in the authorization process, and it holds required information about the authorization process.

- Constrained Layer

RS and C are lies in a constrained node have to execute access control tasks, because they are unable to control complicated tasks of any authorization process requests. Also, they are considered as actors of this layer due to the possibility of unstable network connectivity. Every constrained device is completely linked with a less constrained one, thus will handle the limitation in this layer.

- Organization Layer

In the real world, specific entities control both of C and R. These entities are called Client Organization (COr) and "Resource Organization (ROr) as shown in Figure 7.

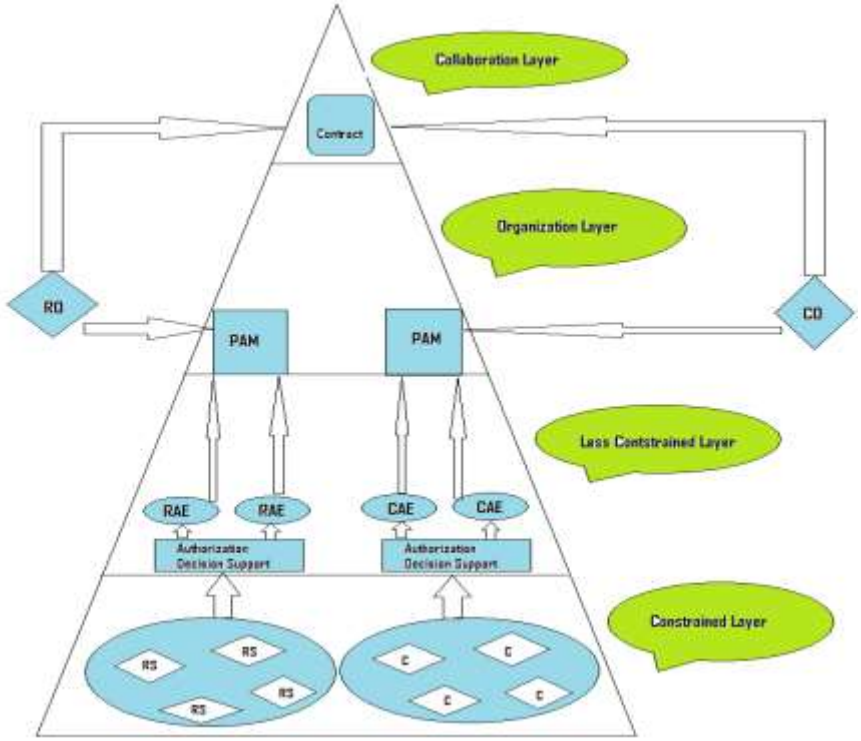

Figure. 7 SIAM Layers.

Consequently, the device's security policy must be defined immediately by the organization itself, and it must structure these devices in specific security domain. The COr is responsible of the entity that request r, and it define security policies for client. Thus, COr has to define authorized S for R.

The resource Organization ROr belongs to the same security domain as R and RS. ROr is in charge of R and RS and thus, must specify the authorization policies for R and decides with whom RS is allowed to communicate. That means that ROr has to configure if and how an entity with certain attributes is allowed to access R. ROr also configures RS and RAE in order to make them belong to the same security domain.

On the client side, the authorized S of R can be subsequently defined by COr, but on the provider side, determining if the entity is allowed to access the requested resource can be achieved by ROr. Before the interaction between ROr and COr takes place, the term of service is used to agree both of them.

- Collaboration Layer

This layer is used to handle the collaborative interaction. It uses an agreement between the organizations in the same domain. According to SIAM format, the access rules is defined. Specific component (called PAM) is located in

organization layer is used to manage this agreement. The RS treats this agreement like all the other rules controlling local communication.

Basically, SIAM begins with the negotiation of collaboration rules just like the related access control rules. Each Org determines which R it will offer to external C, after that it passes them into the PAM. Hence, other Org can contact PAM in case they want to use these resources. To perform that, the agreement of using resources must negotiate both of the COr and the ROr, after that, the COr and the ROr build a connection contract with defined security rules to access R. In fact, this access rules are registered in the collaborated organizations (in their PAM) based on SIAM format. Parallel to this, in the client side, virtual resource is locally created by COr in order to represents remote R, this resource is called R-image. After that, Then COr directlyregisters a rule in its SIAM policy in order to register all of the entities that can use R-image.

6. CONCLUSION

The IoT until now is considered in the first stage of development. Security measures, application of architecture and the foundation have not yet built a standard system for extensive range usage. In the present research, first, a complete review of IoT is done, and a new secure design has been started. Although the IoT is based on the Internet, due to the features of the IoT, those experienced end-to-end security orders and protective measures on the Internet can not immediately afford the end-to-end data security. As the IoT security discussing issues, this research suggests the secure IoT design named SIAM. The common access handle and the identity authentication exclusively operates in the identical layer. SIAM is precisely composed for the IoT and it is understood by a reflection layer that gets used for a deep understanding of the IoT standard as it is applied in the real world. Because of those smart services, contextual information is a head element in choice making therefore only a real-time attention of this information will gain smartness. Because of this purpose, we heightened the "context" notion in order to match the IoT requirements.

REFERENCES

1. Mohamed Abomhara and G.M. Køien, *Security and privacy in the Internet of Things: Current status and open issues*, in *International Conference on Privacy and Security in Mobile Systems (PRISMS)*. 2014, IEEE: Aalborg, Denmark.
2. Ko, M. and C. Dorantes, *The impact of information security breaches on financial performance of the breached firms: an empirical investigation.* Journal of Information Technology Management, 2006. 17(2): p. 13-22.
3. Syafrizal, M. *ISO 17799: Standar Sistem Manajemen Keamanan Informasi*. in *Seminar Nasional Teknologi 2007 (SNT 2007)*. 2007.
4. H. A. Kruger, S. Flowerday, and L. Drevin, *An assessment of the role of cultural factors in information security awareness*, in *Information Security South Africa (ISSA)*. 2011: Johannesburg, South Africa.
5. Whitman, M. and H. Mattord, *Management Of Information Security, Course Technology.* 2008.
6. Von Solms, R. and S.B. von Solms, *Information Security Governance: a model based on the direct–control cycle.* Computers & Security, 2006. 25(6): p. 408-412.
7. Risk, I., *Enterprise risk: Identify, govern and manage IT risk.* Retrieved from, 2009.
8. Whitman, M.E. and H.J. Mattord, *Readings and cases in the management of information security.* 2005.
9. Elky, S., *An introduction to information systems risk management.* 2006.
10. Miorandi, D., et al., *Internet of things: Vision, applications and research challenges.* Ad Hoc Networks, 2012. 10(7): p. 1497-1516.
11. Abdmeziem, R. and D. Tandjaoui, *Internet of Things: Concept, Building blocks, Applications and Challenges.* arXiv preprint arXiv:1401.6877, 2014.
12. Abu-Elkheir, M., M. Hayajneh, and N.A. Ali, *Data management for the internet of things: Design primitives and solution.* Sensors, 2013. 13(11): p. 15582-15612.
13. Abowd, G., et al. *Towards a better understanding of context and context-awareness*. in *Handheld and ubiquitous computing*. 1999: Springer.
14. Bernardos, A.M., P. Tarrio, and J.R. Casar. *A data fusion framework for context-aware mobile services*. in *Multisensor Fusion and Integration for Intelligent Systems, 2008. MFI 2008. IEEE International Conference on*. 2008: IEEE.

15. Li, X. and S.B. Yoo. *Extended role-based security system using context information*. in *Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on*. 2008: IEEE.
16. Martin, D., C. Lamsfus, and A. Alzua. *Automatic context data life cycle management framework*. in *Pervasive Computing and Applications (ICPCA), 2010 5th International Conference on*. 2010: IEEE.
17. Ramparany, F., et al., *An open context information management infrastructure-the IST-Amigo project*. 2007.
18. Floerkemeier, C., M. Lampe, and C. Roduner. *Facilitating RFID development with the accada prototyping platform*. in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on*. 2007: IEEE.
19. Floerkemeier, C., C. Roduner, and M. Lampe, *RFID application development with the Accada middleware platform*. IEEE Systems Journal, 2007. 1(2): p. 82-94.
20. Zeng, D., S. Guo, and Z. Cheng, *The web of things: A survey*. Journal of Communications, 2011. 6(6): p. 424-438.
21. Riedel, T., et al. *Using web service gateways and code generation for sustainable IoT system development*. in *Internet of Things (IOT), 2010*. 2010: IEEE.
22. Roman, R., et al., *Key management systems for sensor networks in the context of the Internet of Things.* Computers & Electrical Engineering, 2011. 37(2): p. 147-159.
23. Davies, R., *The Internet of Things Opportunities and challenges*. 2015, European Parliamentary Research Service. p. 8.
24. Stolpe, M., *The internet of things: Opportunities and challenges for distributed data analysis.* ACM SIGKDD Explorations Newsletter, 2016. 18(1): p. 15-34.
25. Zhang, B., Z. Zou, and M. Liu. *Evaluation on security system of internet of things based on fuzzy-AHP method*. in *E-Business and E-Government (ICEE), 2011 International Conference on*. 2011: IEEE.
26. Mayer, C.P., *Security and privacy challenges in the internet of things.* Electronic Communications of the EASST, 2009. 17.
27. Salman, T. and R. Jain, *Networking Protocols and Standards for Internet of Things.* Internet of Things and Data Analytics Handbook, 2015: p. 215-238.

AUTHORS PROFILE