International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:10, 2018

Security of Internet of Things: Challenges, Requirements and Future Directions

Amjad F. Alharbi, Bashayer A. Alotaibi, Fahd S. Alotaibi

***Abstract*—** The emergence of Internet of Things (IoT) technology provides capabilities for a huge number of smart devices, services and people to be communicate with each other for exchanging data and information over existing network. While as IoT is progressing, it provides many opportunities for new ways of communications as well it introduces many security and privacy threats and challenges which need to be considered for the future of IoT development. In this survey paper, an IoT security issues as threats and current challenges are summarized. The security architecture for IoT are presented from four main layers. Based on these layers, the IoT security requirements are presented to insure security in the whole system. Furthermore, some researches initiatives related to IoT security are discussed as well as the future direction for IoT security are highlighted.

***Keywords*—**Internet of Things, IoT, IoT security challenges, IoT security requirements, IoT security architecture.

I. Introduction

THE emerging approach Internet of things (IoT) aims to connect many devices or daily objects over the internet network with or without human involvement towards creating a more creative environment. The definition of the IoT is always evolving following the continuous change of ideas and technology attached to it. Consequently, some IoT definitions were provided by several sources and researchers. Where Gubbi et al. (2013) define the IoT without standard communication protocol restriction as

> "Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications" [9].

However, ubiquitous computing, sensing technologies, data storage and analytics, pervasive computing, embedded devices, Radio Frequency Identification (RIFD) technology and visualization all these technologies merged in order to make up the IoT environment.

The IoT vision was proposed by Abomhara and Koien (2014) as

> "allow people and things to be connected any- time, anywhere, with anything and anyone, ideally using any path/network and any services" [1],

so IoT seeks to put intelligence into our daily objects to the formation a creative environment.

IoT has tremendous opportunities to performed in various application domains such as Industrial domain, medical and healthcare domains, smart city domain, smart grid, mobility and transportation domain, public safety, environment monitoring domain, etc. Indeed, the result of this interconnection of a huge number of devices, network transmission, data as well as the expanding of IoT application several challenges will be raised such as security and privacy issues. Where security and privacy issues considered as IoT fundamental challenge that needs to be faced in order to support the IoT vision.

The purpose of this paper is to survey the current research effort in IoT security challenges and provide some research initiatives to address those challenges as well as discusses the security requirements in order to support IoT realization in addition to suggests some future research directions.

The remains paper organized as follows. In Section II, presents the literature review. In Section III, discusses some of IoT security threats and challenges. In Section IV, describes the security requirements in IoT architecture. In Section V, presents some researchers Initiatives in the context of IoT Security Issues. In Section VI, presents a discussion and hints for future research. In Section VII, concludes the paper.

II. Literature Review

There are many researches that have been done related to the topic of the present paper. In this section, there is a complete presentation of the most important points when examining security and privacy issues in Internet of Things. These points include; security and privacy threats, security architecture, security requirement, and the challenges occur in this field.

Many studies have mentioned that there are several open challenges that cannot be solved up till now. Abomhara and Køien (2014), examine many barriers and challenges attached to IoT which still being faced and need to be overcome such as assuring interoperability, a business model realization in which hundreds of millions of objects can be linked to a network, security and privacy challenges, such as entities authentication and authorization, trustworthiness, and end-to-end security. Handling such challenges will be the focus of networking research so suggest the research direction to develop a new framework that handle global ID schemes, identity encoding

Amjad F. Alharbi is a Master student at King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: amjad018@gmail.com).
Bashayer A. Alotaibi is a Master student at King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: balotaibi0115@stu.kau.edu.sa).
Fahd S. Alotaibi is an assistant professor with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: fsalotaibi@kau.edu.sa).

or encryption, identity management, authentication as well create global directory lookup and detection services for IoT applications with diverse identifier schemes. However, the authors concluded that powerful security models are required in order to realize IoT technology [1].

There is another classification of security and privacy challenges of IoT that is presented by Fink et al. (2015). They have stated that there are two main challenges; scientific and technical as well as social and regulatory. Another great challenge in IoT that should be also put into consideration is creating a standard security stack similar to the network stack, with standard interfaces and degrees of assurance. They have added that there are some vulnerabilities of internet protocols and lack of powerful mathematical analysis tools which lead to expect a quickly growing set of challenges which are associated with the adoption of IoT systems. For social effect of these technologies, it is difficult to reach [8].

Another point of view that is presented by Strazdins and Wang (2015) shows that there are two main challenges; security challenges and privacy challenges. They have summarized these open challenges and presented their view. When dealing with security challenges, they have discussed authentication and authorization, key distribution and management, safe data transmission, data storage and safe processing, protection against Denial-of-Service attacks, and global laws. Similarly, when they talk about privacy challenges, they have discussed it from certain points; privacy of passive users, privacy preferences, identity control, and business needs. Then they have proposed "to borrow the 'peer approval' scheme from social networks" as a part of authentication system [18].

While Borgia (2014) review a major challenge in different IoT aspect including security and privacy area as locate and relate to all IoT layers, where those challenges require to be faced in order to support IoT realization. Some security requirements were identified that have to be satisfied within IoT applications besides possible solutions to achieve them. The author concludes that there are many open issues stay need suitable solutions [6].

In Weber and Boban (2016), there is a focused discussion on security challenges that are related to implementation of IoT. They have mentioned that there are major challenges and some potential problems that must be put into consideration and require solving before huge application of the IoT which include; confidentiality and privacy, security, heterogeneities management, network capacities limitations, processing and management and of huge amount of data to assure valuable information and service also to assure data integrity and confidentiality [22].

In Nia and Jha (2016), there is a summary of the several attacks against security of IoT along with countermeasures in a level-by-level way as well as the two emerging security challenges that include: exponential increase in the number of weak links because of IoT-based services rely on compact battery powered devices with limited storage and computation resources, and unexpected uses of data which collected by Internet-connected sensors [16].

Farooq et al. (2015) have analyzed the security issues and challenges in each architectural layer. They have presented a reliable architecture for the IoT security which will assure confidentiality of data privacy and security [7].

Ukil et al. (2011) authors consider an IoT security requirement for the embedded devices by assuming network security in secure side. Some of embedded security attacks were highlighted such as "war driving" which attacks unsecured wireless node, many embedded systems are capable to "side-channel" attacks and "third wave of hacking" that involve network, wired computer as well as intelligent devices. In addition, "In-Vehicular" as one of the embedded devices security challenges in which car electronic devices being a suitable goal for manipulations and attacks. Consequently, the embedded security solution was presented in order to address such attacks such as some encryption algorithms, detected hardware and a number of research initiatives such as secure socket layer (SSL) which consider as security protocol treatment [20].

Andrea et al. (2015) study provide a unique classification method to address IoT security challenges and issues, this classification is based on data security as the most significant aim in IoT security. It was built according to IoT layers and it's classified as four layer attacks: physical, network, software and encryption attacks. Moreover, the necessary security countermeasures were provided as a future direction to address these attacks with a view to giving an exemplary layered protection for each layer. It's worth mention that, others propose that "This classification could be used as a framework to categorize attacks, as well as to guide the secure deployment of IoT systems" [2].

Kumar et al. (2016) study and summarized the current security methods according to IoT layers with its limitations in which some of them are not implemented yet or they need to be addressed. Consequently, security framework was proposed as a solution to some those limitations. In the recommended framework, the vulnerability of IoT to threat can be calculated by using Threat Index (TI) in which is calculated based on some parameters from IoT environment. Hence, IoT security performance can be identified and notified to the user. Moreover, the comparison between TI and index threshold help the IoT provider in obtaining knowledge about the current security state as well as in increase or decrease the controls from technical, policy and legal perspective [13].

Kumar and Patel (2014) have provided a survey in which they summarize the security threats and privacy concerns of IoT at different layers. Additionally, they have identified some open issues related to the security and privacy that need to be addressed by research community to make a secure platform for the future of IoT [12].

According to Sicari et al. (2015), requirements of privacy and security have a great function in IoT which is characterized by heterogeneous technologies. Those requirements are authentication and confidentiality of data, trust and privacy between things and users, access control inside the IoT network, and the execution of security and privacy rules and policies. Those requirements, to great extent, are mentioned by most researchers when dealing with such a topic. The main

contribution of this survey is its reviewing of all related security aspects and its including of many references on such a subject [17].

Pan Wang et al. (2016) review the security requirements and IoT security challenges beside provide a framework of IoT security requirements in which security requirement and some potential threats provided in the four layer IoT architecture in terms of general device's security, application security, communication security and network security. Additionally, discuss security solutions for different enabling technologies [21].

Work in, Li et al. (2011) proposes the general architecture of IoT trusted security system, it has been proposed based on previous research in the trusted computing and trusted network area as well as IoT characteristics and security requirements. Consequently, define the usefulness of the proposed structure as to enhance effectively security defense ability in IoT, in which such architecture can be able to realize the integration of trusted (user, perception, terminal, agent) module, decrease the possibility of network safety risks, solving the practical needs of users, manage diverse information security resources and the trusted extension of the IoT functions. Furthermore, the author indicated to the need for further study in order to resolve security problems [15].

A survey was offered by Gupta and Shukla (2016) focused on the security aspects of IoT. Authors discuss different open IoT challenges and security issues in terms of privacy policies which is need to be enforced for each IoT application or infrastructure, security attacks, backdoor and use of wireless sensor networks. It is worth mention that, discuss some of initiatives that related to the adoption of security within IoT dimension. Moreover, examine the design guidelines for any security mechanism that should be considered in order to provide confidentiality, integrity and authentication [10].

III. IOT Security Threats and Challenges

As we know that Internet of Things environment contains from various field of each: software, object, hardware and information interconnected over networks. Security and privacy are essential for each: devices, network and data domain in order to realize an IoT secure environment. Indeed, there are several security challenges that need to overcome and this survey provide some of security and privacy challenges related to object, data, network and IoT Architecture.

A. Authorization and Access Control

The attacker can easily cause damage the system through preventing the access to IoT related services as well they can modify and delete the data through unauthorized access in which could be a deadly for the systems. Consequently, there is a need to address easy access control issues. However, in order to establish a secure connection among number of devices and services authorization and access control are essential. Authorization determine the identification of the object while access control intends controlling the access to resources through granting or denying according to broad criteria, typically authorization is realized through the use of access control [13], [1], [7].

B. User Privacy and Confidentiality

One of the important issues in the field of IoT security is user privacy where the participation in IoT systems will putting their privacy at risk, where often people are not informed about which kind of personal information they are showing plus which their daily activates become tracked. Some important challenges need to be considered and fulfilled such as:

- Privacy of data as well as data sharing and management.
- Standards to manage users and objects identity.
- The need to develop privacy technologies and the related laws.
- Business needs may contradict with user privacy needs so it is important to take into consideration protect the individual privacy when addressing the business needs.
- The need for simpler exchange of critical, protected and confidential information as well as confidentiality need to be a fundamental part of IoT design.
- User should be able to give app permission in order of control their shared information which is called (user preferences). Strazdins and Wang (2015) stated that "Langheinrich [14] uses the term (privacy broker) to describe a third party who acts as a proxy between the data source and applications.", where the privacy brokers mission is to save the information securely and based on user preferences, decide what the information to be shared with each application [1], [22], [18].

C. Software Vulnerability in IoT

Software vulnerability resulted from the programming bugs which is produced by the developers during the software developments stage, according to this vulnerability a number of backdoor security breaches are accrued. Backdoor is the most IoT security concern, where it can be planted by attackers in a vulnerable device to control it. In addition to that product makers can easily deploy backdoor for testing purpose, where this type of testing can be easily cause backdoor security breaches [10].

D. IoT Security Threats

1) DOS Attacks

Denial-of-service attacks (DoS) and Distributed Denial-of-service attacks (DDoS) both of them is an attempt to make the service or network resource unavailable to its users. Where this attempting performs by disrupting the network connection between users and service provider or through the issuance of a large amount useless requests that cause a denial of service.

Most IoT devices are unprotected to resource enervation attacks due to low memory capabilities plus poor computation resources. There is a huge number of DoS attacks which can launch against IoT, such as jamming channels, consumption of computational resources such as disk space, bandwidth, memory, or processor time, and disruption the configuration information. Recently DoS attacks have become advanced, where it offers a smoke screen to hold attacks toward hack the

defensive system plus user data privacy while deceiving the victim in believing that the real attack is appearing somewhere else [18], [1], [7].

2) Attacks on Embedded Devices

IoT embedded devices are vulnerable to several attacks, some of embedded security attacks such as (war driving) which attacks unsecured wireless node, many embedded systems are capable to (side-channel) attacks and (third wave of hacking) that involve network, wired computer as well as intelligent devices. In addition, (In- Vehicular) as one of the embedded devices security challenges in which car electronic devices being a suitable goal for manipulations and attacks.

Embedded security solution was presented in order to address such attacks such as some encryption algorithms, detected hardware and a number of research initiatives such as secure socket layer (SSL) which consider as security protocol treatment [20].

3) Attacks on Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) plays a significant role in IoT where it's transmits data reliably from the sensor node to its destination. The security issues related to the wireless sensor network are: DDOs attacks, Sybil attack, spoofed attacks, Sinkhole Attack, worm hole attacks, false node, node malfunction, message corruption and traffic analysis. These threats and attacks resulted in packets drop, node manipulation resulted in present many identities for one node and network unavailable to the users [7], [10].

4) Eavesdropping Attacks

This kind of attack consider as the most common form of data privacy attack but recently it's become one of security threats in wireless ad hoc networks since most of the adversary attacks involve eavesdropping [1], [18].

IV. Security in IOT

A. IoT Security Architecture

Many researches have been conducted in order to provide a suitable security architecture that is well-defined and can be applied to achieve confidentiality of the data security and privacy [7].

There are four main security layers as shown in Fig. 1 [19]:

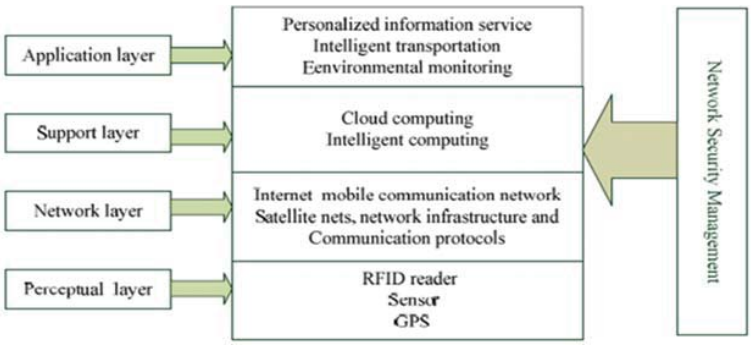

Fig. 1 IoT security architecture

1) Perceptual Layer

The perceptual layer considered as the most important layer. It is also called (recognition layer). This layer collects the whole types of information via physical equipment. Furthermore, it recognizes the physical environment. This information consists of different properties of objects and environment condition. For physical equipment, it consists of RFID reader, the whole types of sensors, GPS and the other different equipment. The most important element in the perceptual layer is sensors since they represent the physical world in the digital world [19].

Perceptual layer is concerned about collecting information, controlling object and perception of object [11].

This layer includes various sorts of data sensors such as RFID and Barcodes or any other types of network sensor. The main objective of that layer is to realize the specific objects and work with its obtained data from the actual world with the support of its particular sensors [7].

2) Network Layer

Network layer is the second level. It is the layer that is in charge for transferring information and data from the perceptual layer, initial processing of information, classification, and finally polymerization. Transferring information within network layer depends on different main networks which includes mobile communication network, internet, wireless network, satellite nets, communication protocols, and network infrastructure. These are the most important elements for exchanging information between devices [19].

Network layer is mainly involved in access world for perceptual layer, perception of information storage and transmission, as well as application layer which provides the other relative works [11].

This layer concerns mainly about transmitting the collected information which is gained from the perceptual layer to any type of information processing system via different communication networks such as Mobile Network, Internet, or any other types of trustworthy network [7].

3) Support Layer

Support layer is the third level. This layer establishes a support platform that can be used for the application layer. Therefore, the whole types of intelligent computing powers are

arranged on this support platform. This is achieved via network grid and cloud computing. Consequently, support platform is an important part in combining the application layer up and the network layer down [19].

Support layer empowers all types of business services and recognize intelligent computation and processing data [11].

This layer includes information processing systems which carry automated actions that are depend on the results of data that processed and link the system with the database that provides storage capabilities to the data collected. Support layer is considered services-oriented that confirms same service kind between the different connected devices [7].

4) Application Layer

The terminal and highest level is the application layer. This layer plays an important role in providing the personalized services based on the users' need. Through this layer, users are able to access IoT by using television, personal computer or mobile equipment [19].

Application layer is related to different applications from RFIDs tracking tag to the smart homes, that are accomplished by some standard protocols and service-composition technologies [21].

This layer recognizes different IoT practical applications that are based on the users' needs and various types of applications such as smart home, smart transportation, and smart hospital [7].

B. IoT Security Requirements

IoT security must combine the security of the entire system crossing the perceptual layer, network layer, support layer, and application layer [11].

For each layer, there are certain security requirements which presented in the following.

1) Perceptual Layer

Authentication and confidentiality of information transmission between the nodes are required. But before achieving authentication and confidentiality, there should be a process of key agreement before doing the data encryption since the safety measures are required. For solving this difficulty, lightweight encryption technology is important to use. This technology consists lightweight cryptographic algorithm and lightweight cryptographic protocol. Protecting sensor data is also needed [19].

For doing authentication, the cryptographic hash algorithms are used. Their benefit is to provide digital signature to the terminals that can prevent any possible attacks. For data privacy, symmetric and asymmetric encryption algorithms are necessary for data privacy [7].

2) Network Layer

In discussing network layer, in order to prevent the illegal nodes, a kind of security mechanism; that is, identity authentication is used. Additionally, establishing data confidentiality and integrality mechanism are needed [19].

By using an appropriate authentication process and point to point encryption, unauthorized access to the sensor nodes can be prevented. After the process of authentication, routing algorithms are employed to confirm the privacy of data interchange between both the sensor nodes and the processing systems. Data integrity methods are used to ensure that the received data which is on the other end is similar to the original one [7].

In network layer, secure transport encryption is important in order to encrypt the transmission in layer [21].

3) Support Layer

To secure the support layer, both secure cloud computing, secure multiparty computation, and antivirus are applied [19].

To avoid the access to any unauthorized user, the process of authentication is used through integrated identity identifications. Various security threats can be solved by applying intrusion detection techniques which produce an alarm in case of occurrence of any attack in the system. This is done because of the continuous monitoring, tracking, and keeping a log of the intruder's activities [7].

4) Application Layer

In application layer, there are two aspects to solve the security problem. The first aspect is the authentication and major agreement across the heterogeneous network and the other aspect is protection of user's privacy. Additionally, it is necessary to use education and management, particularly password management to achieve information security [19].

The requirements of such a layer depend on the applications. To maintain application, there are certain security requirements are needed:

> "remote safe configuration, software downloading and updating, security patches, administrator authentication, unified security platform" [21].

V. Some Researches Initiatives in the Context of IoT Security Issues

In the IoT security domain, some researchers proposed new security frameworks or provided a unique threats classification which help to overcome these threats and challenges. Some of those works discussed in the following.

A. Classification of IoT Security Attacks

According to Andrea et al. (2015), there is a new unique classification of the well-known attacks on IoT systems. This classification, in comparison to the other classifications, presents how to categorize distinctively the attacks under four types; Physical, Network, Software and Encryption attacks. From the physical perspective, the IoT system can be attacked. It can also be attacked from within its network, or from its applications on the system. Finally, it can be attacked on encryption schemes. By using different existing network technologies, IoT is operated. These technologies include; Wireless Sensor Networks, RFIDs and Internet. Therefore, it is required to find an appropriate categorization of the attacks in order to cover all various types of threats. Consequently, better counter measurements can be improved for securing IoT. Table I shows the classification of the attacks [2].

TABLE I
CLASSIFICATION OF IOT ATTACKS

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Chanel Attacks
RF Interference	RFID Spoofing		
Node Jamming	RFID Cloning	Spyware and Adware	Cryptanalysis Attacks:
Malicious Node Injection	RFID Unauthorised Access		a) Ciphertext Only Attack
Physical Damage	Sinkhole Attack		b) Known Plaintext Attack
Social Engineering	Man In the Middle Attack	Trojan Horse	c) Chosen Plaintext or Ciphertext Attack
Sleep Deprivation Attack	Denial of Service		
Malicious Code Injection on the Node	Routing Information Attacks	Malicious scripts	
	Sybil Attack	Denial of Service	Man In the Middle Attack

B. Proposed Security Framework to Address the Current Security Methods Limitations

Kumar et al. (2016) study and summarized the current security methods according to IoT layers with its limitations in which some of them are not implemented yet or they need to be addressed which is shown in Tables II and III. Consequently, security framework was proposed as a solution to some those limitations as well as the implementation of that framework will enhance the IoT reliability and robustness against a set of known attacks [13].

In the recommended framework in Fig. 2, the vulnerability of IoT to threat can be calculated by using Threat Index (TI) in which is calculated based on some parameters from IoT environment. Hence, IoT security performance can be identified and notified to the user. Moreover, the comparison between TI and index threshold help the IoT provider in obtaining knowledge about the current security state as well as in increase or decrease the controls from technical, policy and legal perspective.

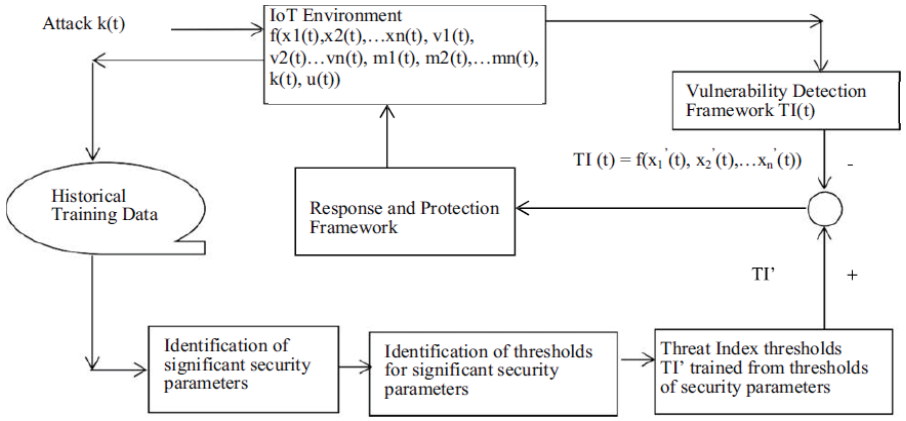

Fig. 2 Recommended security framework

In Fig. 2, the function (x1(t), x2(t), . . . xn(t), v1(t), v2(t) . . . vn(t), m1(t), m2(t), . . . mn(t), k(t), u(t)), represent the IoT. Where xn(t) represents the significant attack sensible network parameters, vn(t) represents the network parameters which are insignificant to node vulnerability representation, mn(t) represents mobility parameters, k(t) represents the attack furthermore u(t) represents control input.

C. Proposed Security Model for IoT

Babar et al. (2010) has proposed a security model for IoT. In order to deal with protection issues in the IoT, interrelated and integrated perspective on privacy, security, and trust can provide an input for such protection issues. Thus, a cube structure has been chosen as a modeling mechanism for privacy, security, and trust in the IoT. This cube has three dimensions that show the intersection between them. The proposed cube is considered as an ideal modeling structure that can be used describe the combined elements of security, privacy, and trust for IoT. IoT access information, which is required to accept or refuse access request, is not complicated but also combined in nature. This is the result of a high level of interconnection between people, things, and services. Therefore, it becomes obvious that the structure and kind of information that is needed to accept or refuse such an access request is complicated. Additionally, it must address and deal with the IoT issues which include; security (authorization), privacy (respondent), and trust (reputation). This is shows in Fig. 3 [4].

D. Privacy-Preserving IoT Security Framework

Bernabe et al. (2014) have proposed privacy preserving IoT security framework. This framework depends on the security functional group of IoT-A Architecture Reference Model (ARM). Both IoT security framework and the IoT-A proposal draw great attention to privacy preserving, contextual management and the security when sharing data within IoT

Communities and Bubbles. To achieve this goal, the framework shows innovative security and privacy mechanisms which combine two new security components: The Group Manager and the Context Manager. The basic components of the security framework with the basic interactions among them are shown in Fig. 4 [5].

1) Authentication and Authorization

The authentication component helps authenticating the user and the smart object which depend on the given credentials. It lets the real identity to be bind to the subject. Consequently, what resulted in the authentication process is a confirmation which is used then in the authorization process in order to show that a particular subject was authenticated completely. To deal with the authentication tokens, SAML protocol is implemented in this framework.

This framework deals with some complex ways of performing authentication by confirming privacy and minimum disclosure of the attributes. This type of alternative privacy-preserving way of authentication can be managed in the framework by the Identity Management Component.

Access Control component is the component that make authorization decisions that depend on access control policies. Therefore, the policies decide which appropriate actions that subjects like smart object and user or groups like communities of bubbles are allowed to implement over a target resource such as IoT Service under specific conditions.

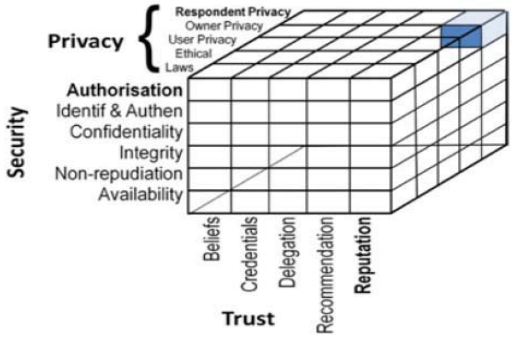

Fig. 3 Security model for IoT

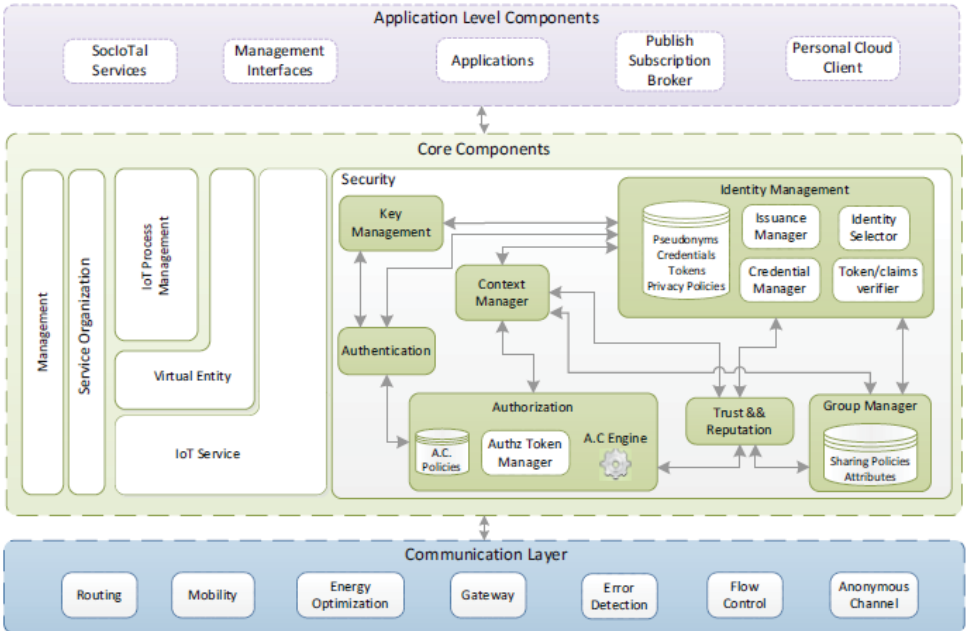

Fig. 4 Security IoT framework based on ARM

2) Identity Management

The Identity Management component is the component that manages the identities of the smart objects and users. This component is responsible for privacy concerns in order to control credentials from users or smart objects in a way of privacy-preserving.

The credential Manager module of the Identity Management system can manage and store the credentials that are utilized by subjects to gain information from an IoT services.

The Token/Claims Verifier module is directed to validate the identity proofs that are used by subjects when they try to access to an IoT service.

3) Group Manager

The group manager component is the component that is responsible for sharing information, in a high secure and private way, with the groups of communities and bubbles that covers specific set of identity attributes values. These specific sets of attributes are presented by attribute sharing policies that are affected by context information where the shared data is performed. This component manages opportunistic bubbles by using of Attribute based encryption mechanism.

4) KEM

KEM is the abbreviation of the Key Exchange and Management which is a component that helps peers who are participated in a communication in the process of constructing a security context, like setting up tunnels for a security communication. This component includes cryptographic key exchange and give interoperability between the peers to find an agreement concerning the security functions to use for the communication. In this framework, there is a focus on the KEM component that are linked with the keys management in the privacy preserving Identity Management System and the Group Manager by means of the CP-ABE cyphering scheme.

5) Context Manager

The Context Manger is defined as the key components in the framework. It preserves the context that is continuously being produced and checked by various context enablers. The Context Manager can hide details about information gathering mechanisms which are used by the context enablers, such as Indoor Localization enabler to get device positions in buildings.

6) Trust and Reputation

The Trust and Reputation component is the component that enables to build an accurate IoT environment where the users can interact with different IoT services and other smart objects in a reliable way. It makes the other components of the security framework to take decisions on security and privacy part based on the quantified trust scores which are used to manage and share data and to evaluate the level of social interaction between users who are in a bubble. This component interacts with the Context Manager to get behavioral information about users, smart objects, IoT services and bubbles and calculate the trustworthiness of a certain entity.

E. Multimedia Traffic Security Architecture for the Internet of Things

1) Multimedia Traffic Classification and Analysis

Zhou and Chao (2011) design a media-aware traffic security architecture to simplify various multimedia applications and services to be available in the Internet of Things environment, by taking on the consideration both of multimedia traffic characteristics, security service and the Internet of Things. Consequently, the proposed architecture designed based on a novel multimedia traffic analysis and classification for handling the heterogeneity of various networks and applications [23].

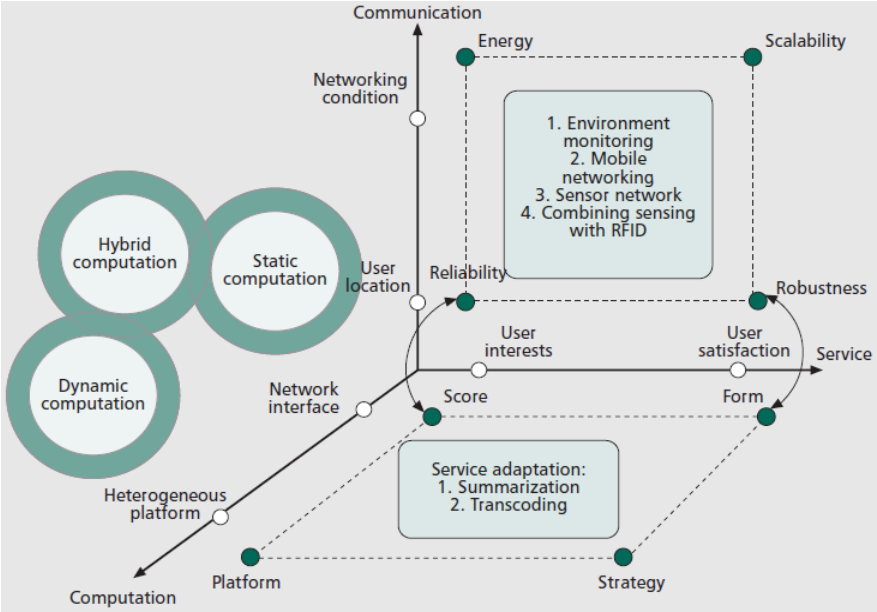

Fig. 5 Multimedia traffic classification and analysis in IoT context

As shown in Fig. 5, multimedia traffic classified into three categories: computation, communication and service in which analyzed them based on that categories.

a. Computation Traffic

This type of traffic over IoT can be processed via mobile agents or sink nodes where there can be a significant impact on computation traffic through the sequence visitation of mobile agent to selected secure nodes. However, computation traffic can be classified to:

- Static computation: The source node determines the computation state of mobile agent before it's dispatched.
- Dynamic computation: The agent autonomously decides the source nodes, and according to the current network conditions the dynamic route or resource allocation is decided.
- Hybrid computation: The sink nodes decide the set of source nodes, while the source-visiting sequences are processed by the mobile agents.

TABLE I
EXISTING SECURITY METHODS AND THEIR LIMITATIONS (PART 1)

Method/Author/Layer	Issues it addresses	Solution	Limitations
RFID Tags (Radio Frequency ID) / Aggarwal et al., [4] (Physical Layer)	Not being able to connect devices	RFID tags can be installed/embedded into smart objects to allow fast communication between devices	While RFID tags are useful for providing security, they are also very prone to hacking as more and more RFID banking applications are becoming susceptible to "RFID hacking"
Identity Management Framework Method / Horrow et al., [1] (Network Layer)	Authenticating data that travels between the device and the cloud	Place an Identity Manager and Service Manager on the devices	The protocols to develop the method have not yet been implemented
ITS Security Methods and Standards for Efficiency – Risk Analysis / Zhao et al., [7] (Network Layer)	Address threats to the ITS or Intelligent Transportation System (i.e. smart transportation)	A public key infrastructure is used in that certificate authenticating (CA's) are used for managing and monitoring security credentials for the network nodes on ITS to devices to prevent data from being interrupted	Technology is still being developed
Authentication and Access Control / Lui et al., [2] (Network Layer)	Fixes loopholes in device security and data integrity	A user requests authentication to access a device, things ask for permission to do so from a "Registration Authority", RA approves devices to send user a question, if response is OK, user is authenticated access to the device	Systems are still very vulnerable to Man in the Middle attacks and Eavesdropping attacks
Security Middleware / You-guo and Ming-fu [6] (Network Layer)	Provides security to Intelligent home systems and communication devices	Uses Entity identification, Secure Storage, Security Audit, Data encryption / decryption, digital signature / verification to secure communication between devices	Middleware is an upcoming trend, it's not yet widely integrated or used
AAL / A. Dohr et al., [10] (Perception Layer)	Safe lifestyle for the elderly people	Keep In Touch (KIT) through smart objects and technologies such as NFC, RFID and Closed Loop Hierarchy	Fails to address the security and privacy issues, though they identify security, privacy and reliability as the main needs of the intended users of AAL.
Cyber Sensors / Liu et al., [8] (Perception Layer)	Lack of data output from physical objects/lack of real time data	Cyber sensors that capture data from physical objects can later be used to perform actions or real – time event response	Some of the technology for the sensors does not yet exist
PKI – Product Key Infrastructure / Li et al., [3] (Perception Layer)	Threats involving node security	Nodes are authenticated by an "offspring node" that sends a decryption key when the node is safely transmitted. Offspring node still continues to be improved and developed.	Encryption is not fast
SMC/Sventek [11] (Perception Layer)	Management and measurement of resources in a ubiquitous computing environment	An SMC (Self-Managed Cells) model which is composed of policy, discovery and role services	Policy services vaguely touch upon the authorization and authentication issues but do not address any other security and privacy issues
ASM/Reijo M. Savola et al., [16] (Perception Layer)	Identifies security objectives and threats in data integrity and adapts to environmental and censored changes that it detects utilizing the security metrics.	ASM comprises of four steps: continuous monitoring, analytics and predictive function, decision making, and metrics based adaptive security models. Sensors are analysed to gather information about the devices surroundings & environment. Very successful in hospitals	The high level security management mechanism does not provide details on the security metrics and the security objectives it tries to solve. Sensors can fall subject to interference from other electronic devices.
DSM/Jafari et al., [12] (Application Layer)	Security metrics for eHealth information systems	For the development of security metrics, they propose five elements that deal with security analysis and policies in general	Fail to address the methods for the identification, collection, computation or the application of the security metrics to address the security issues and objectives.

TABLE II
EXISTING SECURITY METHODS AND THEIR LIMITATIONS (PART 2)

Game Theory /Cox and Balasingham [9] (Application Layer)	The attack of various varying complex systems	Method of attacking systems to develop better security strategies.	Prototyping is not yet complete. So not clear how the system will handle varying complex systems.
Preference Based Privacy Protection Method / Tao and Peiran [5] (Application Layer)	Issues in data privacy	A third party entity evaluates the user's security and privacy preferences and reports it to the service provider that gives the user an appropriate security level based on its sensed preferences before it connects the device to the Internet of Things.	The security mechanism and levels at which to set privacy still require more development as the Internet of Things is fairly new
CCM/Weiss et al. [13] (Application Layer)	Security metrics model based on risk assessment approach	In their model, the security is quantified in terms of incident and asset loss.	Availability and attainability of the data is a challenge to measure security metrics
SMSC/Pierre de Leusse et al. [14] (Application Layer)	Scalable security model for IoT infrastructure	Scalable security enhancement system of the SMC model for distributed resources	This generic model needs to validated for specific applications and security objectives
ASTM/Abie, H. [15] (Application Layer)	System that adapts to changing environment dynamically and anticipating unknown threats	Adaptive learning technique by changing the internal parameters and the dynamic change to the architecture of security systems	This abstract model needs to be validated against dynamic scenarios of application domain and the unknown threats and failures.

b. Communication Traffic

The core components of IoT communication function are sensor networks which composed of some sensing nodes that can be collaborate with RFID systems to complete the communication function, where RFID systems consists of diverse readers and RFID tags and each tag is described by a unique identifier and applied to various objects. Actually, the result of collaborate remote sensing technologies in passive RFID systems can increase the availability of different multimedia traffic types in the IoT environment. Moreover, energy efficiency, reliability, scalability and robust- ness are the objectives of designing a proper multimedia traffic.

c. Service Traffic

Service traffic includes two parts, the score which is mean the degree of user interest in multimedia traffic and form which indicate the content features on a specific device. According to Zhou and Chao (2011) the data was classified into three categories: preference data, capability data and situation data. In addition, there are two techniques used to multimedia traffic adaptation summarization and transcoding. From data size perspective, multimedia summarization means the summarizing of media service in a short one that can be seen on a short timescale while multimedia transcoding means transforming the content from one media type to another, so the content can be efficiently transferred into a specific communication status or suitably processed at a particular device [23].

2) Proposed Media-Aware Traffic Security Architecture

Zhou and Chao (2011) design a novel Media-Aware Traffic Security Architecture to meet the information security requirements of the multimedia traffic classification as discussed above by taking in the consideration traffic security strategy and performance criteria [23].

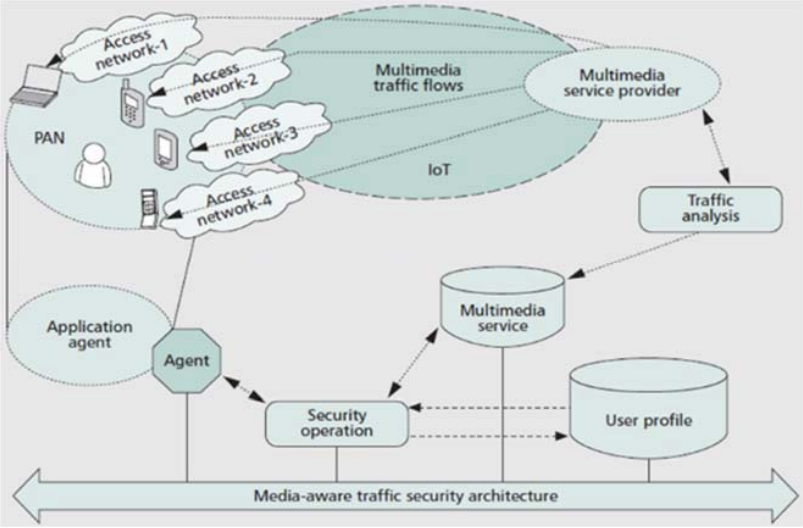

Fig. 6 The framework of the proposed paradigm for implementing MTSA

The designed architecture (MSTA) as shown in Fig. 6 defined as a development of information security framework where multimedia traffic and contents embedded into the proposed architecture. MSTA consist of four major components Key Management, Batch Rekeying, Authentication plus Watermarking.

a. Key Management

Zhou and Chao (2011) propose a new key management schemes into three classifications: (service control, user control, and flow control), by using two criteria the multimedia traffic and whether the scheme is scalable or non-scalable. Where the scalability in the context of IoT key management relates to the ability in providing a wider group of multimedia contents without any previous knowledge [23].

b. Batch Rekeying

Periodic batch rekeying provides a good trade-off between computation complexity and security improvement, Zhou and Chao (2011) list three suggested modes of operation to provide different multimedia application needs as the following [23]:

- Periodic batch rekeying: The key server address each of join and leave requests periodically in a batch.
- Periodic batch leave rekeying: The key server dealings with each join request directly in order to reduce the new user access delay to the IoT.
- Periodic batch join rekeying: The key server deals with each leave request directly in order to reduce the exposure to users who have issued but handles join requests in a batch.

c. Authentication

User authentication cover the following methods:

- Access control: a list of access control for the authorized hosts or excluded was maintained by multimedia server to determine whether it is permitted to join the service group or not by checking its ID in the list when a user sends a join

request.
- Ability certificates: include information about host identity and series of rights generally it is issued by a designated certificate authority. Actually, it is used for user authentication and give him the rights to access multimedia data.
- Mutual authentication between the server and the user by means of encryption. In fact, authentication multimedia regarded as a difficult problem in the telecommunications heterogeneous safe. Thus, there are three levels of multimedia.
- Validation can be used depends on the various types of multimedia applications and network resources as:
- Ratification Group: provides a guarantee that the packets transmitted by the registered user or server.
- Source Authentication: Provides a guarantee that the packets transmitted by the registered users.
- Individual sender authentication: provides guarantees for the identity of the registered users groups.

d. Watermarking

The requirements of watermarks using in multimedia applications:
- The Identification of multimedia content origin require a single watermark embedded into the content at the server.
- In multimedia applications, we need a unique watermark based on the identity or location of the recipient in order to tracing the illegal copies.

Copyright protection is one of the challenging problems in IoT, where all users in a network group receive the same watermarked content if a copy of this content is illegally distributed then it can be difficult to detect who is responsible for this action. In a homogeneous network, such a problem can be overcome by embedding a unique watermark for each user.

VI. Discussion and Future Directions

Axelrod (2015) conclude that

> "The security of application software incorporated into IoT devices as well as the security of the communications software and networks that connect these devices to the Internet are seriously lacking" [3],

and according to this security lacking a worthy future researches are required for all IoT security challenges in order to obtain the desired security level as well as achieve an effective IoT realization for each businesses and individuals.

Currently, there is a need to develop global standards for IoT security and privacy in addition to establish control and governance mechanisms in order to authorize applying the standards. Moreover, must develop policies, legal frameworks and regulations appropriate to assure stabilized development for secure technologies.

In order to Safe data transmission, lightweight encryption algorithms are required according to the IoT nodes finite resources as well as safe protocols that provide adaptive network reconfiguration in order to protect the transmission channel quality. On the other hand, lightweight cryptosystems and security protocols that demand minimum computational power considered as one of IoT security challenges which require research efforts. There is a need to research in risk estimation, further authentication and techniques for detect snooping for each security architecture layer as discussed in Section IV.*B.* Furthermore, there is a suggestion to develop a new framework that handle global ID schemes, identity encoding or encryption, identity management, authentication as well create global directory lookup and detection services for IoT applications [1], [3], [7], [10], [18].

One of the IoT security grand challenges is creating standard security stack with a class of assurance as well standard interface like the network stack. Fink et al. (2015) recommend the research to attempt face this challenge in order to contribute in end-to-end solutions which is required from the technical standpoint [8]. Kumar et al. (2016) identify and mention some capabilities that need to be added in the future to the existing security methods which shown in Section V.*B* as the following [13]:
- Fit the public key infrastructure in the IoT framework.
- Save the IoT from privacy threats as well as recognize privacy parameters, requirements and the mechanism to estimate privacy Threat Index.
- Assure the security issues of the physical level are addressed.
- Develop models for threat and estimate threat index for Eavesdropping and Man in the Middle attacks.
- Carry out cyber sensors which attract data from physical objects in order to calculate threat index aimed at implement actions or response to real – time event.
- To ensuring full end-to-end security there is a need to develop methods to assure the security in transport layer and IPSec.

VII. Conclusion

The IoT technology makes major changes in our life style and presents a new and innovative ways in the internet development. It refers to the communications between different objects over the network. Such objects, should be identify uniquely and determine how it will be represented virtually in the infrastructure of the internet. The rapid progression in the IoT environment introduces invisible opportunities for the communication which lead to change the networking concept as well as it introduces many threats and challenges against security and privacy of users or things.

This survey summarized the IoT security current challenges and threats that need to be addressed and presented the IoT security architecture from four basic layers which include: perceptual layer, network layer, support layer, and application layer. Based on this IoT security architecture, IoT security requirements presented to successfully secure the entire IoT system. In addition, some researches work and future direction discussed in order to overcome the current security threats and challenges.

As a suggestion, proper rules and policies must be carefully developed. Also, the research communities must be focus on these security threats and challenges to come up with some effective countermeasures for the future of IoT development.

REFERENCES

[1] Mohamed Abomhara and Geir M Køien. Security and privacy in the internet of things: Current status and open issues. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pages 1–8. IEEE, 2014.
[2] Ioannis Andrea, Chrysostomos Chrysostomou, and George Hadjichristofi. Internet of things: Security vulnerabilities and challenges. In 2015 IEEE Symposium on Computers and Communication (ISCC), pages 180–187. IEEE, 2015.
[3] C Warren Axelrod. Enforcing security, safety and privacy for the internet of things. In Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, pages 1–6. IEEE, 2015.
[4] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the internet of things (iot). In International Conference on Network Security and Applications, pages 420–429. Springer, 2010.
[5] Jorge Bernal Bernabe, Jose Luis Hernández, M Victoria Moreno, and Antonio F Skarmeta Gomez. Privacy- preserving security framework for a social-aware internet of things. In International Conference on Ubiquitous Computing and Ambient Intelligence, pages 408–415. Springer, 2014.
[6] Eleonora Borgia. The internet of things vision: Key features, applications and open issues. Computer Communications, 54:1–31, 2014.
[7] MU Farooq, Muhammad Waseem, Anjum Khairi, and Sadia Mazhar. A critical analysis on the security concerns of internet of things (iot). International Journal of Computer Applications, 111(7), 2015.
[8] Glenn A Fink, Dimitri V Zarzhitsky, Thomas E Carroll, and Ethan D Farquhar. Security and privacy grand challenges for the internet of things. In Collaboration Technologies and Systems (CTS), 2015 International Conference on, pages 27–34. IEEE, 2015.
[9] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645–1660,2013.
[10] KrishnaKanth Gupta and Sapna Shukla. Internet of things: Security challenges for next generation networks. In Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on, pages 315–318. IEEE, 2016.
[11] Qi Jing, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: Perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.
[12] J Sathish Kumar and Dhiren R Patel. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11), 2014.
[13] Sathish Alampalayam Kumar, Tyler Vealey, and Harshit Srivastava. Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS), pages 5772–5781. IEEE, 2016.
[14] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In international conference on Ubiquitous Computing, pages 237–245. Springer, 2002.
[15] Xiong Li, Zhou Xuan, and Liu Wen. Research on the architecture of trusted security system based on the internet of things. In Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, volume 2, pages 1172–1175. IEEE, 2011.
[16] Arsalan Mohsen Nia and Niraj K Jha. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 2016.
[17] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76:146–164, 2015.
[18] Girts Strazdins and Hao Wang. Open security and privacy challenges for the internet of things. In 2015 10th International Conference on Information, Communications and Signal Processing (ICICS), pages 1–4. IEEE, 2015.
[19] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, volume 3, pages 648–651. IEEE, 2012.
[20] Arijit Ukil, Jaydip Sen, and Sripad Koilakonda. Embedded security for internet of things. In Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on, pages 1–6. IEEE, 2011.
[21] Pan Wang. The internet of things: a security point of view. Internet Research, 26(2):337–359, 2016.
[22] Mario Weber and Marija Boban. Security challenges of the internet of things. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on, pages 638–643. Croatian Society MIPRO, 2016.
[23] Liang Zhou and Han-Chieh Chao. Multimedia traffic security architecture for the internet of things. IEEE Network, 25(3):35–40, 2011.

Amjad F. Alharbi is a Master student in Computing Information Systems at King Abdulaziz University, Jeddah, Saudi Arabia. She has done some researches in E-Commerce, Internet of Things and Decision Support Systems.

Bashayer A. Alotaibi worked as IT technician at Umm Al-Qura University, Saudi Arabia. She is now a master student in Computing Information Systems at King Abdulaziz University. Bashayer has done some researches in Total Quality Management, Internet of Things Applications and she looks forward to conduct research in the field of Information Systems Security.