# Security and Privacy in the Internet of Things: Current Status and Open Issues

Mohamed Abomhara
Department of Information and Communication Technology
University of Agder
Grimstad, Norway
Email: mohamed.abomhara@uia.no

Geir M. Køien
Department of Information and Communication Technology
University of Agder
Grimstad, Norway
Email: geir.koien@uia.no

***Abstract*—The Internet of Things at large will foster billions of devices, people and services to interconnect and exchange information and useful data. As IoT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. Credible, economical, efficient and effective security and privacy for IoT are required to ensure exact and accurate confidentiality, integrity, authentication, and access control, among others. In this paper, the IoT vision, existing security threats, and open challenges in the domain of IoT are discussed. The current state of research on IoT security requirements is discussed and future research directions with respect to IoT security and privacy are presented.**

## I. Introduction

The overall IoT context will consist of billions of individuals, individual devices, and services that can interconnect to exchange data and useful information [1]. Due to swift advancements in mobile communication, Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) innovation, things and mechanisms in IoT can potentially collaborate with one another anytime, anywhere and in any form [2, 3]. There are many possible application areas thanks to these smart things or objects. The major IoT target is the formation of smart environments and self-conscious/ autonomous devices: smart transport, smart items, smart cities, smart health, smart living, and so on [4, 5].

In terms of business, IoT represents tremendous prospect for different types of organizations, including IoT applications and service providers, IoT platform providers and integrators, telecom operators and software vendors [6]. According to some estimates, over 30 billion connected things with more than 200 billion intermittent connections [7] will generate approximately EUR714 billion in revenue by 2020 [8]. Many vertical segments are expected to experience a double-digit growth in upcoming years. Among the most prospective vertical application domains are consumer electronics, automotive industries, and healthcare, as well as intelligent buildings and utilities.

With the rapid increase in IoT application use, several security and privacy issues are observed. When nearly everything will be connected to each other, this issue will only become more pronounced, and constant exposure will literally reveal additional security flaws and weaknesses. Such limitations may subsequently be exploited by hackers, and in a statistical sense all exposed flaws and weaknesses may be abused in an environment with billions of devices [9].

However, in the absence of solid security in place, attacks and malfunctions in the IoT may outweigh any of its benefits [10]. Scalability factors and various restrictions on device capabilities also mean that traditional cryptography mechanisms, security protocols, and protection mechanisms are unavailable or insufficient [11].

The baseline security must be robust and the security architecture must be designed for long system life cycles (>20 years), something indeed challenging. Dealing with large device populations further makes it understandable that some devices will be compromised. Therefore, new methodologies and technologies ought to be developed to meet IoT requirements in terms of security, privacy and reliability [12].

The rest of the paper is organized as follows. In section II an overview of the IoT vision, architecture, application and supporting technologies is provided. Section III identifies some of the attacker models and threats, provides an outline of existing IoT security challenges and describes the security requirements in the IoT. Section IV presents a summarization of the state-of-art in research state of current technologies. Finally, in section V future research directions are discussed and the paper is concluded.

## II. The IoT Vision

The IoT vision is to revolutionize the Internet, to create networks of billions of wireless identifiable objects and devices, communicating with each other anytime, anyplace, with anything and anyone using any service. The increasing enhanced processing capabilities of RFID technologies, wireless sensor networks (WSNs) and storage capacity at lower cost may create a highly decentralized common pool of resources interconnected by a dynamic system of networks.

Through IoT architecture, intelligent middleware will be capable of creating dynamic maps of the physical world within the digital/virtual sphere by applying high temporal and spatial resolution and combining the characteristics of ubiquitous sensor networks and other identifiable things. Figure 1 shows the symbiotic interaction among the real/physical, digital, and virtual worlds with society [13].

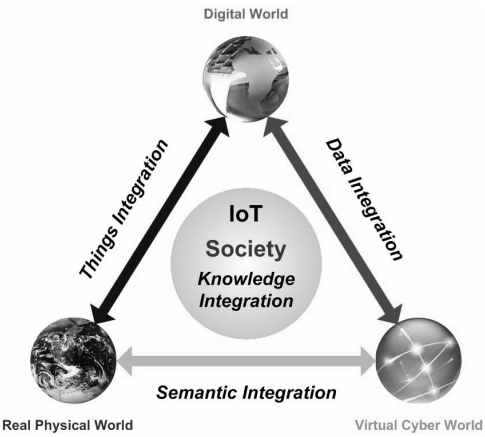


Fig. 1. Internet of Things - a symbiotic interaction among the real/physical, the digital, virtual worlds and society *(Source [13])*

In fact, communications in the IoT will take place not only between devices but also between people and their environment as presented in Figure 2. All individual objects of our everyday life such as people, vehicles, computers, books, TVs, mobile phones, clothes, food, medicine, passports, luggage, etc., will have at least one unique identification allowing them to correspond with one another. Furthermore, since these objects can sense the environment, they will have the capability to verify identities and communicate with each other, such that they will be able to exchange information and become means for understanding complexity, and may often enable autonomic responses to difficult scenarios without human involvement.

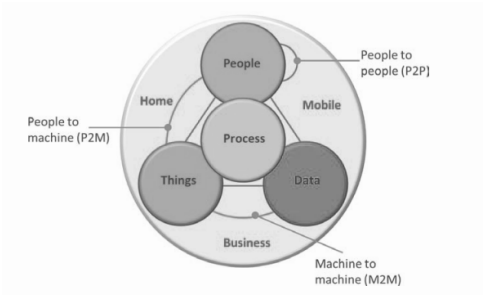


Fig. 2. Internet of Everything *(Source [7])*

The IoT systems will yield tangible business benefits. Once many of these advantages are achieved, such as decentralizing business processes, each thing will have the capacity to interact individually and build up a distinctive life history of its activities and interactions over time. Also possible will be high-resolution management of assets and products, improved life-cycle management and better collaboration between enterprises.

### A. IoT Architectures

Implementing IoT necessitates an open architecture based on several layers to maximize interoperability among heterogeneous systems and distributed resources. There are various research articles on studies of different IoT architecture instances. For example, Debasis and Jaydip [3] showed that IoT is founded on architecture consisting of several layers, from the field data acquisition layer at the bottom to an application layer at the top. Such layered architecture is to be designed in such a way that the requirements of various industries, enterprises, societies, institutes, and governments can be met. Internet layers serve the purpose of common media for communication, the access gateway layer and edge layer contribute to data capturing, while the application layer is responsible for data utilization in applications. In another example, in [14] Chen and others indicated that IoT architecture can be primarily divided into three layers: the perception layer, which assumes information collection, the network layer, for information transmission, and the application layer to realize recognition and perception between objects and objects, and people and objects, and to perform an intelligence function.

Moreover, there are numerous other projects funded by universities and various government bodies for studying the requirements of IoT architecture with the aim to provide an architectural reference [15, 16].

Architecture standards should comprise well-defined abstract data models, interfaces and protocols, together with concrete bindings to neutral technologies in order to support the widest possible range of humans, software, smart objects or devices, operating systems and programming languages [17].

### B. IoT Application Domains

Enabling objects to interrelate in our everyday living and working environments makes many applications possible through the elaboration of information gathered from surroundings. The IoT facilitates the development of numerous applications, either closely or directly applicable to our present existence, of which only few are currently deployed. Some of the more significant examples of IoT applications are categorized into the following domains: personal and social, enterprises and industries, service and utility monitoring, and mobility and transportation [5].

*1) Personal and social domain:* The applications falling in this category permit users to interact with their surroundings (home and work) or with other people to maintain and build social relationships [2].

*2) Mobility and transportation domain:* Vehicles and even roads, with power processors, actuators and sensors, are becoming instrumental to providing suitable transportation information by collecting important data about traffic control and guidance [3, 18]. Traffic Information Grid (TIG) [19] and Intelligent Traffic Information Service (ITIS) [20] are some of the more successful transportation applications in the IoT.

*3) Enterprises and industries domain:* Activities involve financial or commercial transactions between companies, industries, organizations and other entities including manufacturing, logistics, service sectors, banking, financial governmental authorities, intermediaries, etc. [13].

*4) Service and utility monitoring:* This domain usually deals with the protection, monitoring and development of all

natural resources, from agriculture and breeding, to recycling, environmental management services, energy management, and so on.

### C. Supporting Technologies

The advanced development of technologies like communication capabilities, sensors, smart phones, cloud computing, network virtualization and software will enable items to connect with each other all the time, everywhere [7]. The basic concept behind IoT is to interconnect any product in the physical world with the digital world. Several technologies support the concept of IoT, as follows:

*1) Identification technologies:* Wireless Sensor Networks (WSN) and Radio-Frequency Identification (RFID) are expected to play a key role as enablers of identification technology in IoT [2, 6, 13, 21].

*2) Networks and communication technologies:* Wire and Wireless technologies (e.g., GSM and UMTS, Wi-Fi, Bluetooth, ZigBee) will allow billions of devices and services to be connected [22–24]. Scalable and secured architectures designed for IoT network communication are required for secure and reliable wireless communication networks based on wireless identifiable devices and services [3].

*3) Software and hardware technologies:* Research on nano-electronics devices focuses on miniaturization, low cost and increased functionality in the design of wireless identifiable systems [13]. Smart devices with enhanced inter-device communication will lead to smart systems with high degrees of intelligence and autonomy, facilitating the rapid IoT application deployment and creating new services [17].

## III. Security Threats and Challenges in IoT

The three core issues with the IoT are privacy for humans, confidentiality of business processes and third-party dependability. It is acknowledged that in the IoT setting, there are four interconnected, interacting components (people, objects, software and hardware) that communicate over public, untrusted networks. These are bound to be confronted with security, privacy and open trust problems. Therefore, questions regarding users, servers and trusted third parties, as discussed in [25] must be addressed. In such situation, security can be defined as an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures required to protect individual system assets as well as the system as a whole against any deliberate or unintentional threat. All these interactions must also be secured by one means or another, to ensure data and service provisioning of all significant parties and restrict the amount of incidents that will influence the entire IoT.

The remainder of this section identifies some of the attacker models related to IoT, an overview of existing IoT security challenges and IoT security requirements.

### A. Intruder models and threats

Owing to previous vulnerabilities in conventional internet networks, IoT now faces various passive and active attacks that may easily hinder its functionality and nullify the benefits of using its services. Passive attacks are able to recover information from the network yet do not impact its behavior. However, active attacks directly hinder service provisioning [26]. Threats can be classified into external threats that originate from outside the network and internal threats that originate from within the network [27, 28]. Internal attacks tend to be more serious compared with external attacks since the internal knows valuable and secret information, and possesses privileged access rights. According to Computer Security Institute (CIS) and the FBI, approximately 60 percent to 80 percent of network misuse are originate from the inside network [29, 30]. The different types of threats that target IoT are detailed in the following subsections.

*1) Intruder Model.:* A Dolev-Yao (DY) type of intruder shall generally be assumed [31, 32]. That is, an intruder which is in effect the network (Section 3.4 in [33]) and which may intercept all or any message ever transmitted between IoT devices and hubs. The DY intruder is extremely capable and can even surpass the NSA. But while its capabilities are slightly unrealistic,"attacks only get better, they never get worse" remains to be considered, (a quote attributed to Bruce Schneier). Thus, safety will be much stronger if our IoT infrastructure is designed to be DY intruder resilient.

However, the DY intruder lacks one capability that ordinary intruders may have, namely, physical compromise. Thus, tamper-proof devices are also greatly desirable. This goal is of course unattainable, but physical tamper resistance is nevertheless a very important goal, which, together with tamper detection capabilities ("tamper evident") may be a sufficient first-line defense.

Generally, it will be assumed that our "IoT intruder" has full DY intruder capabilities in addition to some limited physical compromise power. We will presume that the physical compromise attacks do not scale, and that it will therefore only at-worst affect a limited population of the total number of IoT devices. The IoT architecture must consequently be designed to cope with compromised devices and be competent in detecting such incidents.

*2) Denial-of-service attacks (DoS):* This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, the majority of devices in IoT are vulnerable to resource enervation attacks. Moreover, the vast majority of defense mechanisms require high computational overhead, and are subsequently not suitable for resource-constrained IoT. Since DoS attacks in IoT can sometimes prove very costly, researchers have exerted an extraordinary arrangement to distinguish different types of such attacks, as well as devised strategies to defend against them. There is a great number of DoS attacks that can be launched against the IoT, such as jamming channels, consumption of computational resources like bandwidth, memory, disk space, or processor time, and disruption of configuration information (such as node information) [24, 34, 35].

*3) Physical attacks:* This sort of attack tampers with hardware components. Due to the unattended and distributed nature of IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks. [35–37].

*4) Attacks on privacy:* Since the IoT makes large volumes of information easily available through remote access mechanisms, privacy protection in IoT is become increasingly challenging. The adversary need not be physically present to carry out surveillance, but information gathering can be done anonymously with very low risk. The most common attacks on user privacy are as follows [38]:

- *Eavesdropping and passive monitoring*: This is most common and easiest form of attack on data privacy. If messages are not protected by cryptographic mechanisms, an adversary could easily understand the content.
- *Traffic analysis*: In order to effectively attack privacy, eavesdropping should be combined with traffic analysis. Through effective traffic analysis, an adversary can identify certain information with special roles and activities in IoT devices and data.
- *Data mining*: This enables attackers to discover information that is not anticipated in certain databases. This could be a security and privacy issue in IoT, and if information is made available, we are perhaps giving out more than we bargained for? [39, 40].

### B. Security and Privacy Challenges in the IoTs

The Internet of Things is a multi-domain environment with a large number of devices and services connected together to exchange information. Each domain can apply its own security, privacy, and trust requirements. In order to establish more secure and readily available IoT devices and services at low cost, there are many security and privacy challenges to overcome. Among those challenges are:

*1) User privacy and data protection:* Privacy is an important issue in IoT security on account of the ubiquitous character of the IoT environment. Things are connected, and data is communicated and exchanged over the internet, rendering user privacy a sensitive subject in many research works [10, 41]. Although an abundance of research has already been proposed with respect to privacy, many topics still need further investigation. Privacy in data collection, as well as data sharing and management, and data security matters remain open research issues to be fulfilled [42].

*2) Authentication and identity management:* Authentication and IdM are a combination of processes and technologies aimed at managing and securing access to information and resources while also protecting things profiles. IdM uniquely identifies objects, and authentication entails validating the identity establishment between two communicating parties [43]. It is essential to consider how to manage identity authentication in the IoT, as multiple users and devices need to authenticate each other through trustable services. Many such open research issues have been presented, for instance in [17]. In order to identify all things uniquely, an efficient identity management approach should be defined. Mobility, privacy, pseudonimity, and anonymity aspects require deeper analysis and research [42].

*3) Trust management and policy integration:* When a number of things communicate in an uncertain IoT environment, trust plays an important role in establishing secure communication between things. Two dimensions of trust should be considered in IoT: trust in the interactions between entities, and trust in the system from the users perspective [34]. In order to gain user trust, there should be an effective mechanism of defining trust in a dynamic and collaborative IoT environment. The main objectives of trust research in the IoT framework are the following: first, the conception of new models for decentralized trust; second, the implementation of trust mechanisms for cloud computing; third, the development of applications based on node trust (e.g., routing, data aggregation, etc.) [42].

Trust evaluation must be automated and preferably autonomous. There are many proposals for automated trust evaluation, and one of the more interesting is the reputation-based Subjective Logic (SL) approach [44]. The SL approach even permits negative trust (distrust), which is a useful abstraction when communicating trust with human users. Within managed IoT systems it is anticipated for the IoT management entity to be a trust hub for all managed devices. Trust may be transitive between systems but needs to be subject to agreements. One model that potentially works out is the roaming agreement model found in cellular systems, whereby a subscriber can use services in other networks provided that the operators have a roaming agreement in place. Trust will ultimately necessitate a foundation, one element of which is trustworthiness. In our context, a trust device must be able to avoid subversion. The paper “Reflections on Trust in Devices“ [45] further investigates trust in devices from a human perspective and provides critical analysis on the limits of trust in software and hardware. In a post-Snowdon context, this provides food for thought. A good policy framework is desired to incorporate the evaluated trust level and current threat level prior to decision making.

*4) Authorization and access control:* Authorization enables determining if the person or object, once identified, is permitted to have the resource. Access control means controlling access to resources by granting or denying according to a wide range of criteria. Authorization is typically implemented through the use of access controls. Authorization and access control are important in establishing a secure connection between a number of devices and services. The main issue to be addressed in this scenario is making access control rules easier to create, understand and manipulate. Additional information on access control is provided next (Sec. IV).

*5) End-to-End security:* Security at the endpoints between IoT devices and Internet hosts is likewise important. Applying cryptographic schemes for encryption and authentication codes to packets is not sufficient for resource-constrained IoT. For complete end-to-end security, the verification of individual identity on both ends, protocols for dynamically negotiating session keys (such as TLS and IPsec), and algorithms (for example AES and Hash algorithms) must be securely im-

plemented. In IoT with end-to-end security, both ends can typically rely on the fact that their communication is not visible to anyone else, and no one else can modify data in transit. Correct and complete end-to-end security is required, without which, many applications would not be possible.

*6) Attack resistant security solution:* There are diverse types of devices with different amounts of memory and limited computation resources that are connected to the internet of things. Since these devices are susceptible to attacks, there should be attack-resistant and lightweight security solutions available. Mitigation planes should be provided on devices to tackle external attacks, such as denial-of-service, flood attacks, etc.

### C. Security requirement for IoTs

IoT has become one of the most significant elements of the future Internet with a huge impact on social life and business environments. As discussed in section III-A, a larger number of IoT applications and services are increasingly vulnerable to attacks or information theft. To secure IoT against such attacks, advanced technology is required in several areas. More specifically, authentication, confidentiality, and data integrity are the key problems related to IoT security [2, 46]. Authentication is necessary for making a connection between two devices and the exchange of some public and private keys through the node to prevent data theft. Confidentiality ensures that the data inside an IoT device is hidden from unauthorized entities. Data integrity prevents any man-in-the-middle modification to data by ensuring that the data arriving at the receiver node is in unaltered form and remains as transmitted by the sender. Table 1 shows a number of security components influencing IoT security functionality.

Vermesan and Friess [7] discussed security and privacy framework requirements in dealing with IoT security challenges, as follows:

- Lightweight and symmetric solutions to support resource-constrained devices.
- Lightweight key management systems to enable the establishment of trust relationships and distribution of encryption materials using minimum communication and processing resources, consistent with the resource-constrained nature of many IoT devices.
- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.
- Techniques to support (”Privacy by Design”) concepts, including data identification, authentication and anonymity.
- Keeping information as local as possible using decentralized computing and key management.
- Prevention of location privacy and personal information inference that individuals may wish to keep private by observing IoT-related exchanges.

## IV. The research state of current technologies

In this section, we explore the condition of research on IoT security requirements.

An overview, categorization, and analysis of security and privacy challenges in the IoT are given in [34, 47, 48]. It has been identified that the protection of user data and privacy is one of the key challenges in the Internet of Things. It is stated that lack of confidence regarding privacy results in decreased adoption among users and is therefore one of the driving factors in the success of IoT.

Roman et al.[10] contend that for IoT to fully bloom into a paradigm that will improve many aspects of daily life, open problems remain to be addressed in several areas, such as cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and trusted architectures.

Suo et al. [11] presented a brief review of security in the IoT and discussed the research status of key technologies including encryption mechanisms, communication security, protecting sensor data and cryptographic algorithms, and concisely outlined the challenges.

### A. Access Control

In literature, two main access control models have been developed: Role-based access control (RBAC) and Attribute-based access control (ABAC). Beyond classical access control, new models so-called usage control (UCON) [49] and $UCON_{ABC}$ [50] were introduced to encompass traditional access control, trust management and digital rights management. UCON enables finer-grained control over usage of digital objects than that of traditional access control policies and models. Unlike traditional access control or trust management, it covers both centrally controllable environment and an environment where central control authority is not available. UCON also deals with privacy issues in both commercial and non-commercial environments. $UCON_{ABC}$ model extended traditional access controls by including three decision factors of Authorizations, oBligations, and Conditions, hence called ABC [51].

Recently, a new model has been proposed by Parikshit et al. [24]. It presents a novel, integrated approach of authentication and access control in IoT devices and aims to replace existing approaches. Another RBAC model worth considering is the so-called Spatial-RBAC (SRBAC) [52, 53]. which has several advantages in a highly distributed IoT system. It neatly captures the fact that threats and exposure are likely to be geographically mapped.

## V. Summary and Conclusion

### A. Summary

The Internet of Things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols. Physical and virtual things have identities, physical attributes, and virtual personalities, employ intelligent interfaces and are seamlessly integrated into the information network. The vision of IoT is to allow people and things to be connected anytime, anyplace, with anything and anyone, ideally via any path/network and service. Identification technologies such as RFID and related

TABLE I
SECURITY COMPONENTS INFLUENCING IOT SECURITY FUNCTIONALITY

| Component Name | Component Functionality | Security Goals |
|---|---|---|
| Authorization | Access control on Devices and services | Data confidentiality Data integrity |
| Authentication | Authentication of service users and devices users | Authentication Accountability |
| Identity Management (IdM) | Management of identities, pseudonyms and related access policies | User privacy Service privacy |
| Key exchange and Management (KEM) | Exchange of cryptographic Keys | Communication confidentiality Communication integrity |
| Trust management and reputation | service trust level and collecting user reputation scores | service trust service reputation |

tools will be the cornerstone of the upcoming Internet of Things. Smart components are projected to be capable of executing different sets of actions, according to the surroundings and tasks they are designed for. There will be no limit to the actions and operations these smart things can perform; for instance, devices will be able to direct their transfer, adapt to their respective environments, self-configure, self-maintain, self-repair, and eventually even play an active role in their own disposal. The IoT make it possible to develop numerous applications either closely or directly applicable to our present living, such as personal and social domains, mobility and transportation domains, enterprise and industry domains as well as service and utility monitoring domains. In order to make IoT services available with a large number of devices communicating with each other, there are many challenges to overcome. In this paper, the security confrontations related to security services have been discussed, such as authentication, privacy, trustworthiness, and end-to-end security.

In summary, it is concluded that to realize the IoT, stronger security models are required that employ context-related security, which in return will help citizens build trust and confidence in these novel technologies rather than increase fears toward complete surveillance scenarios.

### B. Future directions

According to our survey on IoT security and privacy, a great deal of research is needed in order to make the IoT paradigm become reality. In this section, future research directions are suggested:

- Security and privacy issues should be considered very seriously since IoT deals not only with huge amounts of sensitive data (personal data, business data, etc.), but also has the power to influence the physical environment with its control abilities. Cyber-physical environments must accordingly be protected from any kind of malicious attacks.
- Identifying, classifying and categorizing IoT technologies, devices and services that will drive the IoT development and supporting the the IoT vision.
- Design of architecture standards ought to have well-defined abstract data models, interfaces and protocols, together with concrete bindings to neutral technologies in order to support the widest possible range of human beings, software, smart objects or devices.
- Development of new frameworks that address global ID schemes, identity management, identity encoding/ encryption, authentication as well as the creation of global directory lookup and discovery services for IoT applications with various identifier schemes.

### C. Conclusion

The main goal of this paper was to provide an explicit survey of the most important aspects of IoT with particular focus on the vision and security challenges involved in the Internet of Things. the vision of IoT will allow people and things to be connected anytime, anywhere, with anything and anyone, ideally using any path/network and any services. While Radio Frequency Identification techniques (RFID) and related technologies make the concept of IoT feasible, there are several possible application areas for smart objects. The major IoT targets include creating smart environments and self-conscious/autonomous devices, e.g., smart transport, smart items, smart cities, smart health, smart living, and so on. Numerous difficulties and challenges related to IoT are still being faced. Challenges like assuring interoperability, attaining a business model in which hundreds of millions of objects can be connected to a network, and security and privacy challenges, such as authentication and authorization of entities are introduced. In the next few years, addressing these challenges will constantly be the focus and primary task of networking and communication research in both industrial and academic laboratories.

## REFERENCES


[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, 2013.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[3] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[5] D. Yang, F. Liu, and Y. Liang, "A survey of the internet of things," *ICEBI-10, Advances in Intillegant Systems Research, ISBN*, vol. 978, pp. 90–78 677, 2010.