Internet of Things (IoT): Security and Privacy Threats

Eman Shaikh, Iman Mohiuddin, Ayisha Manzoor
Department of Computer Engineering and Science
Prince Mohammad Bin Fahd University
Al-Khobar, Kingdom of Saudi Arabia
e-mail: {emanshaikh26, iman28198, ayishamazoor18}@gmail.com

Abstract— **Internet of Things (IoT) is used for providing connectivity amongst numerous devices. It is a system where objects that are embedded with a detector technology acts with another object through a wireless communication medium to exchange and transfer information without human interaction. These devices are prone to vulnerable attacks due to the simple and open nature of their networks. Therefore, privacy and security are the biggest concern in this technology. The focus of the security and privacy threats on IoT is crucial to promote the development of IoT. The goal of the paper is to put forward the different security and privacy concerns that an IoT environment is facing and the existing mechanisms used for its protection. The paper mainly focuses on the IoT privacy and security features such as the IAS-octave security requirements, security and privacy threats and the solutions that need to be maintained to avoid these security and privacy threats.**

Keywords - Privacy, security, RFID, WSN, IoT, CSP, ISP, sensor, security requirements, attacks, threats, challenges

I. INTRODUCTION

The Internet of Things plays a major role in every individual's day to day life. It is a service that allows person-to-object, object-to-object or object-to-objects transmissions. The applications of IoT are used in many fields such as environmental monitoring, home automation, transportation, medical and healthcare systems, etc. The evolution of IoT is one of the essential and striking occurrences of the previous time period. Technologies like WSN and RFID tags are evolving with increasing development in the scope of Internet technologies [1]. The combination of these two technologies creates direct communication over the Internet. Consequently, there have been a drastic amount of possible attacks and dangers against the security and privacy of a smart thing. These security and privacy requirements are not yet widely known and without proper protection the IoT devices are more likely to be used and attacked for malicious purposes [2]. Therefore, it is important to understand the threats, challenges, and solutions for both security and privacy.

II. SECURITY AND PRIVACY A PROBLEMATIC SCENARIO

A. Potential Attackers and their Motivations

IoT based systems manage a large amount of information that can be used for various services, thus making the IoT paradigm an interesting target for a multitude of attackers, such as occasional hackers, hacktivists, cybercriminals, etc. The potential attackers may be interested in stealing sensitive information such as, location data, credit card numbers, passwords of financial accounts etc. by hacking into the IoT devices. Furthermore, they may even try to compromise IoT components, such as, edge nodes so as to launch attacks against a third-party entity. Moreover, technology and machines have been rapidly growing leading to threats and privacy issues. Smart device communicates and exchanges data with each other within a network. If any device gets corrupted the whole infrastructure is at risk. Thus, security and privacy in the recent years are of great importance [1]. And there is a necessity to establish some security requirements because for instance, if a machine is hacked, the production can be at stake along with the crucial data involved.

B. Definition of Security in the Scope of IoT

Table 1 summarizes the IAS-octave security requirements. The key difference between a security thing and a security attack is that, a security thing is a thing which meets all of the IAS-octave security requirements, whereas a security attack is an attack which tends to threaten at least one of the IAS-octave security requirements [1].

TABLE 1. DEFINES EACH IAS-OCTAVE SECURITY REQUIREMENTS

Requirement	Definition	Abbreviation
Confidentiality	Ensuring that only authorized users access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
	An ability of a system to confirm	

978-1-7281-0108-8/19/$31.00 ©2019 IEEE

Non-repudiation	occurrence/non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling individuals to control their personal information	P

C. Definition of Privacy in the scope of IoT

Due to the significant increase in the use and efficiency of electronic data processing, these days information privacy has become a key issue. Privacy in the scope of IoT can be classified into three categories: (i) Awareness of privacy risks imposed by smart things and services surrounding the data subject, (ii) Individual control over the collection and processing of personal information by the surrounding smart things, (iii) Awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere [3]. In a smart home scenario, the subject's household or immediate vicinity can be described as the subject's personal sphere and may tend to differ from situation to situation. Privacy tends to vary in perception and requirements depending upon the individual thus leading to an unclear conception of personal information. Therefore, when designing new systems and services careful assessment of the sensitivity of the information involved and the relating user requirements must be taken into consideration.

III. SECUIRTY THREATS

A. Wireless Sensor Network (WSNs):

WSNs are easily prone to IoT security attacks due to the transmission medium used for broadcasting. Some of the major WSN threats are:

1. *Physical Attacks:* A sensor device must be implemented in every object to achieve their full capability. However, it is difficult to physically protect the devices as well as to stop unauthorized physical access. A hacker can make changes to the available data of a node/sensor, thus leading to the functioning of the whole sensor network to be at risk [2].

2. *Node Replication:* In this attack, an existing node identifier of a sensor is copied to the same network as a new sensor that would lead to duplication causing misrouting of packets, recording of false sensor readings, or a network disconnection thereby disrupting a sensor network's performance [4].

3. *Selective Forwarding:* In WSN, it is assumed that all nodes receive messages to the destination. A malicious node selectively forwards packets in this attack. It may simply drop certain messages without forwarding them. It is difficult to identify the attacker as they tend to modify packets which originate from a few specific nodes and the message is then forwarded to the other nodes thereby limiting the suspicion of the malicious node's modifications [4] [2].

4. *Wormhole Attack:* It is a critical attack in which the attacker records packets at some location in the network and then tunnels them to a different location. This process can be carried out selectively. Moreover, when routing control messages are tunneled, routine may be disrupted [2].

5. *Sybil Attack:* This attack was introduced in the context of peer-to-peer networks. It takes place when a computer is hijacked and the hacker claims multiple identities and an adversary can manage to be at more than one place at a time. A single node presents multiple identities in the network which leads to significant reduction of effectiveness of fault tolerance such as distributed storage, disparity and multipath [4].

6. *Sinkhole Attack:* An intruder takes over a node inside the network and tries to attract all the traffic from neighbor nodes. This process can be carried out with the use of the routing algorithm and attracting other nodes. The adversary launches many severe attacks including forwarding the packets selectively, modification of messages or deleting the packets [4] [2].

7. *Service Attack denial or Denial of service attack*: Services are made unavailable to legitimate users and the links of victim are destroyed by flooding them with legitimate-like requests from the attacker, thus leading to denial of all the services sent by legitimate users [2].

8. *Eavesdropping:* The intruder listens to the information during data transmission between the two nodes over a network. Information remains the same but its privacy is compromised. The intruder can use this information against the user [4] [2].

B. Radio Frequency Identification (RFID):

Some types of attacks against RFID technology are as follows:

1. *Physical Data Modification:* Tags are physically obtained by the attacker and then data is altered. Fault induction is used to modify a physical data. Fault induction is a process of modifying data when it is written or processed and can be performed using laser cutting microscopes or small charged needle leading to mismatch between the data stored on the tags and the objects to which these tags are attached. An RFID tag attached to a manufactured product gives incorrect information about the item. The tag traceability reduces due to this attack [2].

2. *Tag Cloning:* The original tag is replaced with a new one and the original tag identifier (id) is copied to it. If there is no physical access protection for the RFID tags, then the attacker can easily replace the original tag with a new one [4].

3. *Tag Swapping*: A popular attack in which the tags of two different products are replaced. It occurs in retail stores where a high-priced tag is exchanged with a low-priced tag so that the high-priced product is purchased at a lesser rate. [4] [2].

4. *Denial of Service Attack:* When an information is requested from a tag by the RFID reader, it receives the identification id of the tag and then compares it with the id stored in its database. Both RFID reader and server database are vulnerable to DoS attack, as a result when this attack takes place, the tag fails to send its identity to the reader. Thus, the connection between the tag and the reader will not be stable and in turn will lead to service interruption a study. [4].

IV. SOLUTIONS FOR SECURITY THREATS

A. Security solutions for Wireless Sensor Networks (WSNs)

Some of the solutions regarding wireless sensor networks are as follows:

1. *Shared Keys:* A security feature which tends to receive a huge deal of concentration in WSNs is the key management area. WSNs are found to be unique in this characteristic due to their size, mobility and power constraints. Traditionally, using one of the many public-key protocols leads to the completion of key establishment. Usually by applying a simple key infrastructure, protection against outsider attacks is taken care

for any network. However, it is known that a global key does not provide any network resilience, and pairwise keys are not a scalable solution [12].

2. Protected Grouping: WSN consists of a large number of small nodes which are compact and automated devices. Sensor nodes are required to bind the nodes together. For completing a particular task, it is important that the group members must be able to securely communicate with each other, even though overall security may also be in use. Exceptions for the solutions are made when more powerful nodes are in charge of protecting the member of static groups [18].

3. Encryption: Sensor networks mostly run in public or wild areas over inherently unconfident wireless channels. Thus, it is insignificant for a device to eavesdrop or even add messages into the network. The traditional way of solving this problem are to adopt techniques such as message authentication codes, symmetric key encryption schemes and public key cryptography [12].

4. Secure Data Aggregation: Sensor networks and data aggregation techniques tend to be vulnerable towards a range of attacks including denial of service attacks. The most important trouble in networks is data traffic which is caused due to the increase in data transfers. In order to decrease the overhead cost and network traffic, sensor nodes aggregate measurements before sending them to the base station. This type of data allures an attacker [19]. The credibility of the generated data will be affected if an adversary has control over an aggregating node and chooses to ignore the report or produces a false report. As a result, the network as a whole must be considered. The main aim in this area is to use resilient functions that shall be able to discover and report forged reports through demonstrating the authenticity of data somehow. However, an enhancement in this area may be still required, such as amount of data, which is generated by interactive algorithm [20] [18].

5. SPINS: Security Protocols for Sensor Networks: SPINS are optimized for resource constrained environments and Wireless communication. SPINS have several building blocks due to which it offers many security properties such as data authentication, data freshness, semantic security, low communication overhead, and replay protection [21].

6. TinySec: Link Layer Security Architecture: TinySec can be included into sensor network applications as they are lightweight and have a general security package, and so it is included in the official TinyOS release. The two special security options that TinySec supports are, authenticated encryption (TinySecAE) and authentication only (TinySecAuth). With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC. During the authentication only mode, TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted [12].

B. Security solutions for Radio Frequency Identification (RFID)

i. Physical method

1) Kill tag:

The principle used for this method is disabling the tag's function to stop tracing the tag and its carrier, this is what is usually done in a supermarket. The advantage of kill command is tag losing. For example, the tag's information will be of no use once an item is sold. It is not convenient for post-sale service and further understanding of the product. Moreover, if the kill identification number (PIN) is revealed, a person with an ill intention may steal from the supermarket [10].

2) Faraday net:

According to the electromagnetic field theory, a container made up of Faraday net conductive material will not be able to enter Faraday net outside a radio wave and vice versa. By placing a tag within a container made up of conductive material most likely prevents the tag from being scanned, i.e. a passive tag cannot receive a signal and an initiative tag cannot send a signal out. Therefore, using the principle of Faraday net can prevent privacy intruder from scanning a tag's information. For example, if a coin is inserted in a RFID tag, by using the principle of Faraday net one can prevent a privacy intruder from scanning it so that no one gets to know the amount of in the user's handbag [10].

3) Stopping tag

The principle behind the use of a special stopping tag is to interfere with anti-collision algorithm which means that the same response data is sent to the reader so that the tag is protected [8].

ii. RFID security protocol

The software security mechanism based on secret code technique are more welcomed by users instead of the hardware security mechanisms that are based on physical methods. Although recently many RFID security protocols have been proposed, most of them have various drawbacks.

In 2003, a lightweight tag authentication protocol was proposed by Vajda etc. It is a balancing solution that balances between performance and security. The attacker may be able to uncover the protocol if he owns plentiful computing resources [11].

Sarma etc proposed a Hash-Lock protocol which uses the metaID to replace the real tag ID so that information does not get traced or leaked. However, an ID dynamic refreshing mechanism is not present. The metaID is kept constant and no changes are made to it. Moreover, the ID is sent by plain text through an unsafe channel. Thus, it is most likely that the protocol might be attacked by a fake name or retransmit [11].

Weis etc proposed a random Hash-Lock protocol which uses a query-response mechanism based on random numbers. The tag ID passed authentication is sent by plain text through an unsafe channel. Thus, the protocol is also likely to be attacked by fake name or re-transmit, and traced. As the data volume that is transferred between the tag and reader is large, the application prospect is not that great [11].

Su etc proposed a LCAP protocol which also is a query-response type protocol. The tag ID is dynamically refreshed after each operation. The protocol only needs two discrete calculations. The complexity of the algorithm is reduced as it cuts the ID into two parts, i.e., left and right. As it consists only of tag ID and one directional Hash function, it very well meets the low-cost requirement of the RFID system. Since the tag ID is sent only if it passes authentication, and is refreshed after each operation, then the LCAP protocol can effectively prevent tracing and information leakage. Tag ID is refreshed after receiving the ID update message and the message having passed authentication upon the termination of each talk. Upon this time, background database has already updated the relevant ID. Although LCAP protocol is a satisfactory authentication protocol for low-cost RFID system, it is not fit for general computing environment for distributed database, as database synchronization is a potential security hidden danger [11].

TABLE 2. WSN SECURITY THREATS AND SOLUTIONS

Threats	Solutions
Physical attack and Reverse engineering	Tamper resistant mechanism
Data integrity problem	Detects security threats in data integrity then adjusts to environment with censored changes detected while exploiting metrics for security
Sybil attacks	Keep tracking the number of clones
Sinkhole attack	By avoiding congestion
Malicious node	By detecting malicious node and distribute separately in blacklist
DDOS attack	Packet marking, filtering and dropping mechanism
Attack on network availability	Secure routing
Eavesdropping	Secure relay communication
Cryptanalysis attack	Enhanced two way user authentication scheme

TABLE 3. RFID SECURITY THREATS AND SOLUTIONS

Threats	Solutions
Forgery	Faraday cage
Tag cloning	Tag identifier authentication; valid identifier is used to clone a tag
Counterfeiting	Two-way authentication protocol
Tracking tags	Ultra-light weight mutual authentication protocol
Killing tag approach	By killing the tags, they are not reused

V. PRIVACY THREATS

A. Identification

Identification denotes the threat of connecting a (persistent) identifier, such as the address and name or a pseudonym of any type, with an individual and information about him. The threat lies in connecting an identity to a specific privacy, violating context and it also activates and facilitates other threats. For instance, profiling and tracking of individuals or collection of different data sources. The threat of identification is presently most prevalent in the information processing phase at the backend services, where huge amounts of data is collected in a central place outside of the subject's control. The main challenge faced in identification is the design of IoT systems which favor local over centralized processing, horizontal over vertical interactions, such that a minimum amount of identifying data is available outside the personal sphere of a user [3].

B. Localization and Tracking

Localization and tracking denote the threat of determining and documenting an individual's location through time and space. Tracking needs identification to bind continuous localizations to one individual [9]. Presently, tracking is possible through different means, such as internet traffic, GPS, or cell phone location. Most of the concrete privacy violations have been identified related to this threat, for instance GPS stalking, disclosure of private information, or generally the feeling of being stalked**.** In the immediate physical proximity, localization and tracking usually does not lead to privacy violations, for instance, anyone in the immediate surrounding can directly observe the subject's location**.** Localization and tracking thus appears as a threat mainly in the phase of information processing when locations traces are built at back ends outside the subject's control. The main challenges faced in localization and tracking is the awareness of tracking in the face of passive information concentration, control of shared location data in indoor environments, and privacy preserving protocols for communication with IoT systems.

C. Profiling

Profiling denotes the threat of collecting or arranging information dossiers about individuals in order to deduce interests by correlation with other profiles and data. The methods of profiling methods are mainly used for personalization in e-commerce (recommender systems, newsletters and advertisements) but also for internal optimization based on customer demographics and interests [9]. Examples where profiling is led to a violation of privacy violation are price discrimination, unsolicited advertisements, social engineering, or erroneous automatic decisions, e.g. by Facebook automatic detection of sexual offenders. Collecting and selling profiles about people is commonly perceived as a privacy violation. These examples show that the profiling threat appears mainly in the dissemination phase, towards third parties, but also towards the subject itself in form of erroneous or discriminating decisions. These approaches can be possibly applied to IoT scenarios but should be adapted from the usual model that assumes a central database and account for the many distributed data sources which are expected in the IoT. This requires considerable efforts for recalibration of metrics and redesign of algorithms, as e.g. recent work in differential privacy for distributed data sources shows. Data collection is one of the primary promises of the IoT and a main driver for its realization. Thus, it is seen as the biggest challenge in balancing the interests of businesses for profiling and data analysis with individual's privacy requirements.

D. Privacy violating interaction and presentation

In this threat, personal details are delivered through a public medium and then is revealed to undesirable individuals. Numerous IoT applications such as the manufacturing, infrastructure, medical and healthcare systems etc need abounding connections within the user. In these systems, it is conceivable that the details are provided to the users with the help of the utilization of smart things in the surroundings. For instance, through approaching lighting techniques and television or desktop screens showing videos. Conversely, users dominate systems in an alternative instinctive methodology with the utilization of smart things in the environment (such as feeling and communicating smart objects). Nevertheless, numerous intercommunications and organizing procedures are intrinsically public. This thus creates a cause to privacy issues when secret information is interchanged between the user and the system. For instance, in smart cities, an individual may question the route to a specific hospital. Such an enquiry should not be replied back (such as displaying the route on a public road can be observed by anyone who passes by the same road) [3].

E. Lifecycle transitions

Privacy is intimidated when smart objects reveal their secret details throughout the alteration of managing domains in their lifecycle. This issue is noticed with respect to the undermining pictures and videos that are usually seen on cameras and other new devices as well. Since privacy contraversions from life cycle are primarily due to the gathered information, this depends on the information level of the IoT reference model. The life cycle of many customer care products is even now designed as buying the product for once continually and the results have not yet progressed. Smart objects can attribute for a more engaging life cycle that will include interchanging, lending, giving and disposing pricelessly. Therefore, we recognize the needs for adaptable results that will clearly constitute some problems. Some life cycle transformations (such as sharing a smart object needs fastening secret details at a temporary stage). The secret details can be unfastened and the actual owner can pursue using the device consistently [3].

F. Inventory attack

This is defined as the uncertified gathering of data regarding the reality and features of personal devices. Interconnection of IoT devices is considered as one important evolving feature of IoT. Smart objects are considered to be inquirable over the Internet with the identification of all the internet protocols. Authorized organizations can query things from all over (like the certified system users and owners) whereas the non-authorized organizations can query and breach this to arrange a detailed record of things at a particular area (such as an office building, public institutional places, industrial area etc). Even though smart objects can easily determine authorized and non-authorized organizations, a fingerprint of these organizations transmission rate and other rare specifications could be utilized to identify their category and representation. With the anticipated escalation of WSNs technology, fingerprinting procedures could also be exhibited submissively (like a secret listener in the locality of a victim's home) [3].

For frustrating the inventory attacks in IoT, we distinguish the two specialized problems as follows: First of all, smart object should be enabled to validate enquiries and respond to those queries by authorized organizations to frustrate agile inventory attacks. Second of all, methodologies that safeguard the wellness against fingerprinting will be asked to protect and prevent passive inventory attacks based on the transmission fingerprint of a smart object [9].

G. Linkage

In this threat, formerly separate system devices are connected together, (such as the gathering of information related to different datas are disclosed which were never disclosed to the formerly obscure sources). The users are ignorant of the superior evaluation and data lost when all the different datas and authorizations are put together. Another example of privacy contravention via linkage is the rapid expansion of unknown data provided [3]. Linkage threats will exacerbate into the evolution of IoT for primarily two reasons. Firstly, a parallel interconnection will finally connect systems from different organizations to generate a diversified system that supplies new services which no single system ever provided on its own. Secondly, a prosperous interconnection of such thing will gradually need an agile interchange of information and maintenance between different individuals.

VI. PRIVACY PRESERVING SOLUTIONS

Several approaches have been suggested for addressing the privacy concerns and privacy considerations of service providers:

A. Cryptographic techniques and information manipulation

Though researchers have spent a lot of years in proposing a novel privacy preserving schemes, cryptography is still the most dominant one in almost all of the current proposed solutions, even though, for most of the obstacles faced, many of the sensors cannot offer adequate security protocols due to the limited amount of storage and computation resources [5].

B. Privacy awareness or context awareness

Solutions for privacy awareness have been mainly focused on the applications of individuals which provide a basic privacy awareness to their users that smart devices, such as wearable fitness devices, smart TVs, and health monitor systems could collect personal data about them. For example, in recent research, a framework called SeCoMan was proposed to behave as a trusted third party for the users as applications might not be trusted enough with the location information that is managed [6].

C. Access control

Access control is one of the viable solutions used in combination to encryption and privacy awareness. This gives users the power to manage their own data. An instance of this approach is CapBAC [7], proposed by Skarmeta, Hernandez, and Moreno. It is essentially a distributed approach in which smart things themselves are allowed to make authorization decisions.

D. Data minimization

The principle of data minimization means that the IoT service providers should limit or reduce the concentration of personal data to what is directly relevant. They should also keep the data only for as long as it is required to fulfill the purpose of the services provided by the technology. There are other suggested solutions that do not fall into the previous four categories, such as hitchhiking. This is a new approach to ensure the anonymity of users who provide their locations. Hitchhiking applications handle locations as the entity of interest. As the knowledge of who is at a particular location is unnecessary, the fidelity trade off is removed [9].

VII. CONCLUSION AND PROPOSED SOLUTION

IoT is an emerging technology that has made significant progress in the standardization of technology. There are tremendous benefits of IoT in the business, academic sectors and as well as for the individuals itself. The information in IoT is transmitted from RFID tags or sensors which carries sensitive information that is protected from any unauthorized access [4]. Hence, security and privacy are very crucial to protect IoT systems. This paper reviews the major threats and their respective solutions in IoT by identifying different areas that are sensitive to security and privacy attacks. Present-day problems must be considered as an enhancing opportunity which includes security intentions at an early development phase and a successful application of security regulated answers at a production phase. As a future perspective to protect IoT, better security frameworks can be developed which can address the privacy issues across all boundaries. Further research is required to develop and design appropriate security mechanisms that are resilient to different types of attacks. Therefore, users, organizations and developers need to come under one roof and find a prominent solution for a secured IoT environment.

However, manipulation of a user's data can be avoided altogether if the user only shares the required information at the required time and discards the rest of his or her information thereby making the process faster, efficient and reducing it from the privacy threats discussed in the paper.

ACKNOWLEDGMENT

The authors would like to thank Dr. Nazeeruddin Mohammed for his assistance and Prince Mohammad Bin Fahd University (PMU) for supporting this paper.

REFERENCES

[1] A. Mosenia and N.K. Jha, (2016, September). "A comprehensive study of Internet of Things." In *Emerging Topics in Computing.* [Online]. 5(4), pp. 586-602. Available: https://ieeexplore.ieee.org/document/7562568 [March 26, 2018]

[2]Md. Husamuddin and M. Qayyu. “Internet of Things: A study on Security and Privacy Threats.” In Second International Conference on Anti-Cyber Crimes (ICACC), 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7905270 [March 26, 2018].

[3] J. H. Ziegeldoorf, O.G. Morcon, and K. Wehrle, (2017, May). “Privacy in the Internet of Things: Threats and challenges.” In *Journal of Computing and Machinery.* [Online]. 7(1), pp. 110–119. Available on: https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf [March 26, 2018]

[4] K. Raju and V. Bapauji. “Internet of Things (IoT): Security and privacy threats.” In IEEE International Conference Robot Autom, 2016. [Online]. Available: https://www.researchgate.net/publication/305302451 [March 26, 2018]

[5] H. Feng and W. Fu. “Study of recent development about privacy and security of the Internet of Things.’ In IEEE International Conference on Web Information Systems and Mining, 2, pp. 91–95, 2010. [Online]. Available: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/5662804/ [March 26, 2018].

[6] A. H. Celdran, F. J. G. Clemente, M. G. Perez and G. M. Perez. “SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications.” In IEEE Systems Journal, 10(3), pp. 1111-1124, 2016. [Online]. Available: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/6718051 [March 26, 2018].

[7] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno. “A decentralized approach for security and privacy challenges in the internet of things.” In IEEE World Forum on Internet of Things (WF-IoT), pp. 67–72. IEEE, 2014. [Online]. Available: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/6803122 [March 26, 2018].

[8] M. Daud, Q. Khan, and Y. Saleem. “A study of key technologies for IoT and associated security challengers.” In International Symposium on Wireless Systems and Networks, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8250042 [March 26, 2018]

[9] N. Aleisa and K. Renaud, “Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion),” unpublished. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1611/1611.03340.pdf [March 26, 2018]

[10] A. Khattab, Z. Jeddi, E. Amini,. And M. Bayoumi. “RFID Security Threats and Basic Solutions.” In *RFID Security: A lightweight paradigm*. Switxerland: Analog Circuits and Signal Processing, 2017, ch. 2, pp. 27-41. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-47545-5_2 [March 26, 2018].

[11] Q. Wang, X. Xiong, W. Tian and L. He. “Low-cost RFID: Security problems and solutions.” In the International Conference on Management and Service Science, 2011. [Online]. Available: https://ieeexplore.ieee.org/document/5998331 [March 26, 2018]

[12] A. Jain, K. Kant and M. R. Tripathy. “Security solutions for Wireless Sensor Networks.” In Second International Conference on Advanced Computing & Communication Technologies, 2012, pp. 430-433. [Online]. Available: https://ieeexplore.ieee.org/document/6168407 [March 26, 2018]

[13] M. Dabbagh and A. Rayes. “Internet of Things security and privacy” in Internet of Things from hype to reality. [Online]. 2017, pp. 195-223. Available: https://www.researchgate.net/publication/309375790 [March 26, 2018]

[14] Harpal, G. Tejpal and S. Sharma. “A survey article on attacks and security goals in Wireless Sensor Networks.” In Second International Conference on Communication and Electronics Systems, 2017, pp. 683-686. [Online] Available: https://ieeexplore.ieee.org/document/8321166 [March 26, 2018].

[15] A. Tyagi, J. Kusshwah and M. Bhalla. “Threats to security of Wireless Sensor Networks.” In Seventh International Conference on Cloud Computing, Data Science & Engineering – Confluence, 2017, pp. 402-405. [Online]. Available: https://ieeexplore.ieee.org/document/7943183 [March 26, 2018]

[16] M. Frustaci, P. Pace and G. Aloi. “Securing the IOT world: issue and perspectives.” IEEE Conference on Standards for Communications and Networking CSCN), 2017, pp. 247-251. [Online]. Available: https://ieeexplore.ieee.org/document/7888545 [March 26, 2018]

[17] Z. Ren, X. Liu, Runguo and T. Zhang. “Security and Privacy on Internet of Things.” Seventh IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017, pp. 140-144. [Online]. Available: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/8076530 [March 26, 2018]

[18] W. Al Shehri. “A survey on Security in Wireless Sensor Networks.” International Journal of Network Security & Its Applications (IJNSA), 9(1), 2017, pp. 25-32. [Online]. Available: http://aircconline.com/ijnsa/V9N1/9117ijnsa03.pdf [March 26, 2018].

[19] M. Saraogi. "Security In Wireless Sensor Networks." pp. 1-12. [Online]. Available:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.5923&rep=rep1&type=pdf [March 26, 2018].

[20] K. Sharma, M.K. Ghose, D. Kumar, R. P. K. Singh and V. K. Pandey. “A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks”. In International Journal of Advanced Science and Technology (IJAST), 17, 2010, pp. 31-44. [Online]. Available: http://modul.repo.mercubuana-yogya.ac.id/modul/files/openjournal/JournalOfDesign/4_263.pdf [March 26, 2018].

[21] Md. A. Hamid, M.d. Mamun-Or-Rashid, and C. S. Hong. “Routing Security in Sensor Network: Hello Flood Attack and Defense” In IEEE ICNEWS, 2006, pp. 77-81. [Online]. Available: http://networking.khu.ac.kr/layouts/net/publications/data/Routing%20Security%20in%20Sensor%20Network%20HELLO%20Flood%20Attack%20and%20Defense.pdf [March 26, 2018].