ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 4, April 2018

A Survey on various IoT Attacks and its Countermeasures

[1] C.Ramakrishna, [2] G.Kiran Kumar, [3] A.Mallikarjuna Reddy,[4] Pallam Ravi
[1][2][3][4] Associate Professor
[1][2][3][4] Dept. of CSE, Anurag Group of Institutions, Hyderabad, T.S., India.

Abstract: The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. Internet-of-Things (IoT) are anywhere in our everyday life. Though, all those advantages can come of enormous risks of confidentiality, security and integrity issues. To provide better security of the IoT devices, several studies have been showed to overcome those problems and find a optimal solutions to exclude those threats. The survey consists of three categories. The first category will explore the most significant disadvantages of IoT devices and its solutions. The second category will present the various types of IoT attacks. The third segment will focus on the Common attacks and countermeasures.

Index Terms— Internet-of-Things (IoT), Attacks, privacy, security, WSN,RFID.

1. INTRODUCTION

INTERNET-OF-THINGS (IoT) is a collection of “things” embedded with electronics, software, sensors, actuators, and connected via the Internet to collect and exchange data with each other. The IoT devices are equipped with sensors and processing power that enable them to be deployed in many environments. Fig. 1 presents a variety of common IoT applications, including smart home, smart city, smart grids, medical and healthcare equipment, connected vehicles, etc. The IoT Key Feautres are artificial intelligence; connectivity; sensors; active engagement; and small device use. IoT key features as stated below:

• AI – IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.

• Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

• Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

• Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

• Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

The fast growth of the number of IoT devices utilized is predicted to reach 42 billion in 2020 with an $9 trillion market [1] as stated in the 2013 report of the International Data Corporation. The difference between IoT and the traditional Internet is the absence of Human role. The IoT devices can create information about individual’s behaviors, analyze it, and take action [2]. Services provided by IoT applications offer a great benefit for human’s life, but they can come with a huge price considering the person’s privacy and security protection.

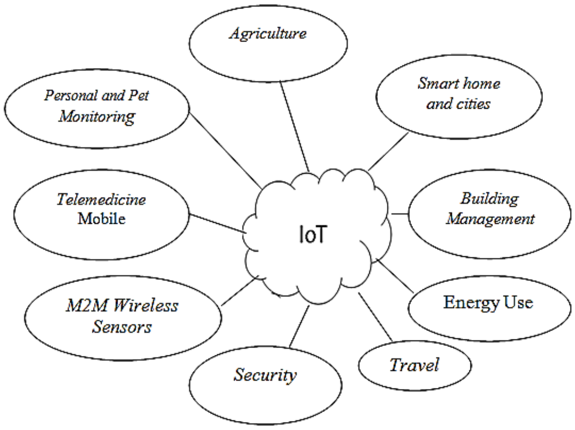

Fig.1 IoT Applications

IoT manufacturers failed to implement a robust security system in the devices, security experts have warned the potential risk of large numbers of unsecured devices connecting to the Internet [3]. B. Lam et al. proposed a New Hampshire-based provider of domain name services, experienced service outages as a result of what appeared to be well coordinated attack [4].Following the never-ending string of disclosures about major data breaches, consumers are wary of placing too much personal data in clouds, with good reason [5].

Granjal et al. [6] analyzed existing solutions for the IoT standardized communication and cross-layer mechanisms whenever applicable. Sicari et al. [7] presented research challenges and the current solutions in the field of IoT security concentrating on the main security issues. Roman et al. [8] proposed an attacker model that was applied to both centralized and distributed IoT architectures.

The present paper is organized as follows. The second aspect presents the most relevant limitations of IoT devices. The third aspect discusses the classification of various types IoT attacks. Finally, we explore the Common attacks and countermeasures.

II. IoT LIMITATIONS

Internet of Things is the interconnection of several physical objects including everything such as home appliances (washing machine, toaster, refrigerator, microwave oven, coffee maker, etc.), mobile phones, laptops, television, etc. All the connected “things” are embedded with sensors, softwares, electronics and Internet connectivity in order to exchange information with each other. The following are the some of the limitation of IoT.

***1. Privacy* –** This is a great concern when it comes to exchanging valuable information regarding anything. Since everything will be connected breaching inside the network would be easy by the hackers. By entering into just a part of network would reveal everything regarding an individual or organization or both .

***2. Safety* –** If a situation comes like a notorious hacker changes your medical prescription and you are supplied expired medicines or those medicinal drugs to which you are allergic to, then there would be a health disaster. Since the consumer that time would be dependent entirely on the technology there would be least probability that he would bother checking anything. The verification today is done manually by the consumer himself but no one knows what will happen later.

***3. Compatibility* –** At present there is no international standard for device compatibility. For example, home based appliances and equipment may be getting problems in connecting with laptops or mobile phones. Also Apple devices don’t accept the connectivity with any other device. Likewise different manufacturers need to agree upon this else people will prefer buying only one brand and there would be monopoly.

Shafagh et al. [9] proposed an encrypted query processing algorithm for IoT. The approach allows to securely store encrypted IoT information on the cloud, and sup-ports efficient database query processing over encrypted data. Specifically, they utilize alternative lightweight cryptographic algorithms that replace additive homomorphic encryption and order-preserving encryption with Elliptic Curve ElGamal and mutable order preserving encoding algorithms, where they made some changes to suit the computation limitations of IoT devices. The system scheme replaces the Web application communication with an end-to-end (E2E) system that stores encrypted data from personal devices on cloud database, and data encryption/decryption is performed at the client-side. The keying material will only reside in the personal device, and the need of a trusted proxy which has access to all the secret keys is eliminated. The system architecture includes three main parties: 1) IoT devices; 2) users; and 3) the cloud. The application data can be stored in the cloud by directly uploading it by the smart device or via a gateway like a wearable device. The paper addressed only some encryption schemes that support the most used queries in IoT data processing. However, the design can be extended to cover more schemes. The experiment results showed an improvement in the time performance compared to existing schemes.

Kotamsetty and Govindarasu [10] proposed an approach to reduce latency for IoT when performing query process-ing over encrypted data by applying latency hiding technique, which consists of breaking down the query results of large size into small sized data sets. This allows computational work to be performed on a set of data while fetching the remaining encrypted information. To decide the appropriate data size to be requested in each iteration in order to minimize the latency, the study proposed an algorithm that starts with an initial data size and adoptively adjust the size to minimize the gap between computation and communication latencies in each iteration. The algorithm has two variants: the first starts with a size that is a fraction of the large query size. In the second variant, the starting size is fixed. The experiment results demonstrated that the proposed approach outperforms existing solutions in terms of latency for queries with larger data size.

Salami et al. [11] proposed a lightweight encryption scheme for smart homes based on stateful identity-based encryption (IBE), in which the public keys are merely identity strings without the need for a digital certificate. This method is known as Phong, Matsuka, and Ogata's stateful IBE scheme. It is the combination of IBE and stateful Diffie-Hellman encryp-tion scheme. To add more efficiency to the proposed scheme and reduce the communication cost, the research study divides the encryption process into key encryption and data encryption, with the focus on the second one, because the size of ciphertexts produced by key encryption is larger than the one resulted from the data encryption.

III. CLASSIFICATIONS ON IoT ATTACKS

We can classify generally five categories of IoT security attacks, namely i)Physical attacks ii)Side channel attacks iii)Cryptanalysis attacks iv)Software attacks and and v)Network Attacks.

i) Physical attacks: These types of attacks tamper with the hardware components and are relatively harder to perform because they requires [12] an expensive material. Some examples are de-packaging of chip, layout reconstruction, micro-probing, particle beam techniques, etc.

ii) Side channel attacks: These attacks are based on a side channel Information that can be retrieved from the encryption device that is neither the plaintext [12] to be encrypted nor the cipher text resulting from the encryption process. Encryption devices produce timing information that is easily measurable, radiation of various sorts, power consumption statistics, and more. Side channel attacks make use of some or all of this information to recover the key the device is using. It is based on the fact that logic operations have physical characteristics that depend on the input data. Examples of side channel attacks are timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks and environmental attacks.

iii)Cryptanalysis attacks: These attacks [12] are focused on the cipher-text and they try to break the encryption, i.e. find the encryption key to obtain the plaintext. Examples of cryptanalysis attacks include cipher-text only attack, known-plaintext attack, chosen-plaintext attack, man-in-the-middle attack, etc.

iv) Software attacks: Software attacks [12] are the major source of security vulnerabilities in any system. Software attacks exploit implementation vulnerabilities in the system through its own communication interface. This kind of attack includes exploiting buffer overflows and using Trojan horse programs, worms or viruses to deliberately inject malicious code into the system. Jamming attack is the one of the ruinous invasion which blocks the channel by introducing larger amount of noise packets in a network. Jamming is the biggest threat to IoT. where a network consists of small nodes with limited energy and computing resources. So it is very difficult to adopt the conventional anti jamming methods to implement over IoT technologies.

v) Network Attacks: Wireless communications[12] systems are vulnerable to network security attacks due to the broadcast nature of the transmission medium. Basically attacks are classified as active and passive attacks. Examples of passive attacks include monitor and eavesdropping, Traffic analysis, camouflage adversaries, etc. Examples of active attacks include denial of service attacks, node subversion, node malfunction, node capture, node outage, message corruption, false node, and routing attacks, etc.

Andrea et al. [13] come up with a new classification of IoT devices attacks presented in four distinct types: 1) physical; network; 3) software; and 4) encryption attacks. Each one covers a layer of the IoT structure (physical, network, and application), in addition to the IoT protocols for data encryption. The physical attack is performed when the attacker is in a close distance of the device. The network attacks consist of manipulating the IoT network system to cause damage. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system. Encryption attacks consist of breaking the system encryption. This kind of attacks can be done by side channel, cryptanalysis, and man-in-the-middle attacks. They also presented a multilayered security approaches to address the IoT structure layers and encryption system vulnerabilities and security issues. Based on the study, to countermeasure the security problems at the phys-ical layer, the device has to use secure booting by applying a cryptographic hash algorithms and digital signature to verify its authentication and the integrity of the software. Also, a new device must authenticate itself to the network before any transmission or reception of data. In addition to that, a device should carry an error detection system, and all of its information has to be encrypted to maintain data integrity and confidentiality. At the network layer, authentication mechanisms and point-to-point encryption can be used to ensure data privacy and rooting security. The application layer can also provide security by means of authentication, encryption, and integrity verification, which allows only the authorized users to access data through control lists and firewalls, in addition to the use of anti-virus software.

Ronen and Shamir [14] introduced a new taxonomy classification for IoT attacks based on how the attacker features deviates from the legitimate IoT devices. The categories are presented in: ignoring, reducing, misusing, and extending the system functionality. The study focused on the functionality extension attacks on smart lights. The paper presented two attacks: the first one consisted of creating a covert channel to capture confidential information from an organization build-ing that implemented smart lights which are connected to the internal sensitive network. The work is done by using an optical receiver that could read the data from a distance of over 100 m by measuring the exact duration and frequency of the small changes in the lights intensity. The second attack showed that an attacker can use those lights to create strobes in the sensitive light frequencies, which can lead to a risk of epileptic seizures. The experiments showed that it is necessary to focus on security issues during the different phases of designing, implementing and integrating of the IoT devices.

a) Layered classification of attacks on the WSN

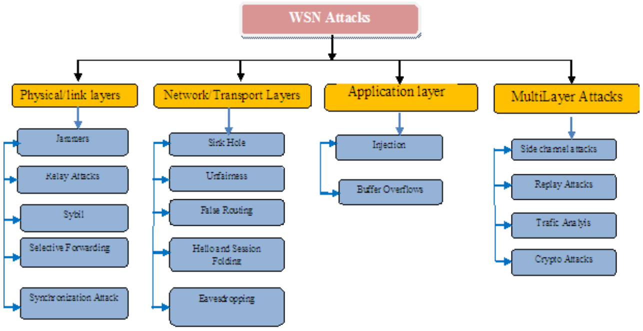

Fig.2. layered classification of WSN attacks

Hence, this classification has allowed us to easily locate each attack and then tackle the security issues according to the actions performed by the attacker. The attacker could be either an active attacker by performing an action that could jeopardize the benefit of the WSN, or a passive attacker whose objective is to eavesdrop the network. In this context, numerous techniques and tools have been developed to deal with WSN security attacks. The most existing attacks [15] and vulnerabilities in WSN, whereas, in the last section, we will suggest some countermeasures against these attacks. In the figure 2 shows the layered classification of WSN attacks.

b) Layered classification of attacks on the RFID

Despite the facilities it offers, the wireless medium used in RFID network has some drawbacks that leave it vulnerable to different types of attacks that target this type of transmission medium. We classified these attacks based on the layer where each attack could be performed.

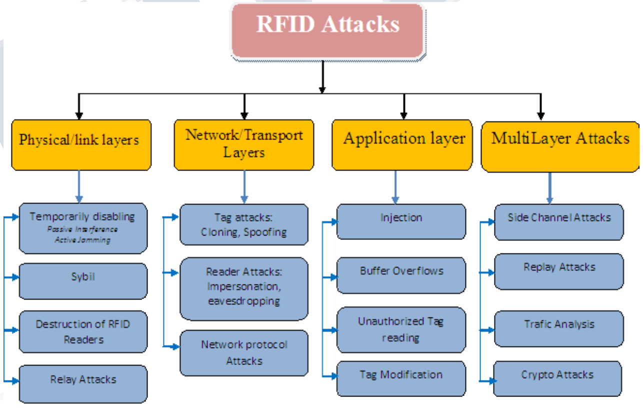

Fig.3. Layered classification RFID attacks

The Figure 3 represents a classification of RFID network attacks. As mentioned above, we discriminate attacks that could be deployed to physical layer, network-transport layer and the application layer, as well as multilayer attacks, which affect more than one layer. According to the functionalities and features of each layer, an attacker chooses a specific attack to carry out. Among these attacks we point out the relay attacks, destruction of RFID readers, Sybil attack and the temporarily disabling passive interference, active jamming as security risks that could be faced on the physical/link layer. Regarding the threats associated to the network/transport layer we find the tag attacks such as cloning and spoofing, the reader attacks like impersonation, eavesdropping and the network protocol attacks. As to application layer several attacks [16]can be considered such as injection, buffer overflows, unauthorized tag reading [16].

IV. COMMON ATTACKS COUNTERMEASURES

This section is an overview of existing countermeasures to enhance security of IoT communication technologies. We identified countermeasures for WSN/RFID combined attacks and countermeasures as shown in Table 1.

Attacks	Counter Measures
Jamming	Regulated transmitted power, Direct-Sequence Spread Spectrum, Direct-Sequence Spread Spectrum, and Hybrid FHSS/DSSS.
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use packet leach techniques.
Replay	Timestamps, one-time passwords, and challenge response cryptography
Trafic Analyis	Sending of dummy packet in quite hours: and regular monitoring WSN network
Evaesdropping	Session Keys protect NPDU from Eavesdropper
Sybil	Trusted Certification. Resource Testing, Recurring Fees, Privilege Attenuation, Economic Incentives, Location/Position Verification, Received Signal Strength Indicator (RSSI)- based scheme and Random Key Predistribution.

Table 1. Common attacks and countermeasures

4.1. Countermeasure against Jamming

4.1.1. Regulated transmitted power

By using low transmitted power, the discovery probability from an attacker decreases [17] .Higher transmitted power implies higher resistance against jamming because a stronger jamming signal is needed to overcome the original signal [17].

4.1.2. Frequency-Hopping Spread Spectrum

Frequency hopping spread spectrum (FHSS) is a way of transmitting radio signals by fast switching a carrier amid many frequency channels, benefitting from the use of a shared algorithm known both to the transmitter and the receiver. FHSS brings forward many advantages in WSN and RFID systems [18].

a) It reduces unauthorized interception and jamming of radio transmission between Tag and Reader in RFID and the nodes in WSN.

b) It deals effectually with the multipath effect. One of the main drawbacks of frequency-hopping is that the overall bandwidth required is much wider than that required to transmit the same data using a single carrier frequency. However, transmission in each frequency lasts for a very limited period of time so the frequency is not occupied for long.

4.1.3. Direct-Sequence Spread Spectrum

Direct-Sequence Spread Spectrum (DSSS) transmissions are performed by multiplying the data (RF carrier) being transmitted and a pseudo-noise (PN) digital signal. This PN digital signal is a pseudorandom sequence of one and one values, at a frequency (chip rate) much higher than that of the original signal. This process causes the RF signal to be replaced with a very wide bandwidth signal with the spectral equivalent of a noise signal; however, this noise can be filtered out at the receiving end to recover the original data, through multiplying the incoming RF signal with the same PN modulated carrier. The first[19] three of the above-mentioned FHSS advantages also apply into DSSS. Furthermore, the processing applied to the original signal by DSSS makes it difficult to the attacker to descramble the transmitted RF carrier and recover the original signal.

4.1.4. Hybrid DSSS

In WSN the Hybrid DSSS communication between nodes represents the hoped anti-jamming measure. In general terms, direct-sequence systems achieve their processing gains through interference attenuation using a wider bandwidth for signal transmission, while FHSS through interference avoidance. Thus Hybrid [18] DSSS develop the solidity to combat the near/far problem, which arises in DSSS communications schemes. Another welcome feature is the capability to adapt to a diversity of channel problems.

4.2. Wormhole Countermeasure

A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. Strictly speaking, the attacker does not need to understand the MAC protocol or be able to decode encrypted packets to be able to replay them. Different papers in literature have developed countermeasures for wormhole attacks. The authors [20] discussed them in two approaches. The first one is related to that Bound Distance or Time, and the second is based in graph theoretic and geometric.

4.3. Replay Countermeasure

In order to defend against replay attacks some simple countermeasures exist such as the use of timestamps, one-time passwords and challenge response cryptography. Nevertheless, these schemes are inconvenient and with doubtful efficiency considering the vulnerabilities to which challenge response protocols are susceptible to. Another approach is the use of RF shielding on readers in order to limit the directionality of radio signals and subsequently the appearance of a ghost. Another approach is based on the distance between the information requestor and the information owner. Implied that the signal-to-noise ratio of the reader signal in an RFID [21]system can reveal even roughly the distance between a reader and a tag. This information could definitely be used in order to make discrimination between authorized and unauthorized readers or tags and subsequently mitigate replay attacks.

4.4. Traffic Analysis Countermeasure

The way to defend against traffic analysis is to control the packet sending rate of every node in the network in such a way that every node sends packets with the same rate [22] . There is another way to defend traffic analysis is to ensure that the external appearance of a packet changes as it moves forward through a multi-hop sensor network. To do this, a cluster key is established among each set of neighboring nodes. The packet destination address, packet type, and packet contents are encrypted by a node, using its cluster key [22] . As a packet moves forward, each node first decrypts the packet and then re-encrypts it, using the cluster key. The current senders address remains in plaintext so that the receiver can choose the correct cluster key to decrypt the packet.

4.5. Countermeasure against Eavesdropping

Communications between WSN nodes and RFID are vulnerable to the eavesdropping because very few nodes and passive tags are using the cryptographic protections. However, due to the short reading range of passive tags , the eavesdroppers need to be the physical proximity of RFID tags, which is a sporadic activity. In order to protect against eavesdropping, data cryptography can prevent these security issues. Presently, sensor networks are supplied exclusively through symmetric key cryptography. The entire network is under risk if only one of its nodes has to be compromised by using symmetric cryptography. It means that the shared secret among those nodes is exposed. Another approach is to use a shared key between two nodes in the whole network. Then, it removes the network wide key. The disadvantage is additional nodes which cannot be added after the deployment process. In a sensor network with n nodes, each node needs to store (n-1) keys.

4.6. Countermeasure against Sybil attacks

There are different methods proposed against Sybil attacks but still there is no general solution to the Sybil attack. A number of approaches for various combinations of environments and attacks have been proposed[23] . The most prominent techniques to resist Sybil attacks are as under.

a)Trusted Certification: is by far the very often cited solution to subdual Sybil attacks. It involves the presence of a trusted Certifying Authority (CA) that validates the one is to one correspondence between nodes on the network and its associated identity.

b) Resource Testing: is the most habitually implemented solution against Sybil attacks, despite it is ineffective for most systems.

c)Recurring Fees or (Recurring Costs) is a variation method of resource examining where resource tests are conducted after certain specific time intervals to impose a specific "cost" on the attacker that is incurred for every identity that he controls. Using recurring costs or fees per identity is more effective to inhibit Sybil attacks than a one-time resource test.

d)Privilege Attenuation: is a technique to mitigate Sybil attack limited to Social Network System (SNS) [24] as an application domain, this technique frequently used in (SNS) despite its disadvantages is only applied to monotonic policies. Significant run-time and storage overhead for generalized extensions of the idea.

e)Economic Incentives: is a general technique used to mitigate Sybil attack, but this method is not efficient because it may encourage Sybil attackers[25]that have no interest in subverting the application protocols, but that are interested in being paid to reveal their presence.

f)Location/Position Verification: this technique is only limited to ad hoc networks. Methods employing this technique make use of the fact that any identities that are projected by any single physical device must be in the same location. Locations are verified using specific methods such as triangulation [26]. So for an attacker with a single physical device, all Sybil identities will be in the same place or will appear to move together

Received Signal Strength Indicator (RSSI)–based scheme: is a technique used to mitigate Sybil attack[27]. It does not deal with existing Sybil nodes in the network, Location calculations are costly. It is limited to Sensor Networks.

Random Key Redistribution: is a technique[28] limited in wireless sensor network but we can use it in other systems like RFID.

5. CONCLUSION

The Internet of things technologies are exposed to different types of attacks. An attacker can attack for different objectives. Attacks are classified based on attacking goals and different OSI layers. In this paper, the most important attacks on WSN and RFID are identified, discussed, and presented in a systematic form to allow their comparison The use of conventional cryptography in the Internet of things is limited or even impossible. In this paper we will explore the most significant disadvantages of IoT devices and further we discussed various types of IoT attacks and its countermeasures.

REFERENCES

[1] IoT Analytics. (2014). Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation. [Online]. Available: https://iot-analytics.com/Internet-of-things-definition/

[2] I. Saif, S. Peasley, and A. Perinkolam. (2015). Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age. [Online]. Available: https://dupress.deloitte.com/ dup-us-en/deloitte-review/issue-17/Internet-of-things-data-security-and-privacy.html

[3] M. Rouse. (2013). IoT Security (Internet of Things Security). [Online]. Available: http://internetofthingsagenda.techtarget.com/ definition/IoT-security-Internet-of-Things-security

[4] B. Lam and C. Larose. (2016). How Did the Internet of Things Allow the Latest Attack on the Internet? [Online].Available:https://www.privacyandsecuritymatters.com/2016/10/howid-the-Internet-of-things-allow-the-latest-attack-on-the-Internet/.

[5] Talkin Cloud. (2016). IoT Past and Present: The History of IoT, and Where It's Headed Today. [Online]. Available: http://talkincloud.com/cloud-computing/iot-past-and-present-history-iot-and-where-its-headed-today?page=2

[6] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for IPv6 enabled wireless sensor networks," in Proc. IFIP Wireless Days, Venice, Italy, Oct. 2010, pp. 1–6.

[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, pri-vacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, Jan. 2015.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Comput. Netw., vol. 57, no. 10, pp. 2266–2279, 2013.

[9] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the Internet of Things," in Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), Paris, France, 2015, pp. 251–253.

[10] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query pro-cessing on encrypted data for the Internet of Things," in Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN), Aug. 2016, pp. 1–7.

[11] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryp-tion for smart home," in Proc. 11th Int. Conf. Availability Reliability Security (ARES), Salzburg, Austria, Aug. 2016, pp. 382–388.

[12] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[13] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in Proc. IEEE Symp. Comput. Commun. (ISCC), Larnaca, Cyprus, Jul. 2015, pp. 180–187.

[14] E. Ronen and A. Shamir, “Extended functionality attacks on IoT devices: The case of smart lights,” in Proc. IEEE Eur. Symp. Security Privacy (EuroS P), Saarbrücken, Germany, Mar. 2016, pp. 3–12.

[15] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

[16] Rieback, M. R., Simpson, P. N., Crispo, B., & Tanenbaum, A. S. (2006). RFID malware: Design principles and examples. Pervasive and mobile computing, 2(4), 405-426.

[17] Zhang, Y., & Kitsos, P. (2009). Security in RFID and sensor networks. Auerbach Publications.

[18] Mpitziopoulos, A., & Gavalas, D. (2009). An effective defensive node against jamming attacks in sensor networks. Security and Communication Networks,2(2), 145-163.

[19] Fang, S., Liu, Y., & Ning, P. (2016). Wireless communications under broadband reactive jamming attacks. IEEE Transactions on Dependable and Secure Computing, 13(3), 394-408.

[20] Maheshwari, R., Gao, J., & Das, S. R. (2007). Detecting wormhole attacks in wireless networks using connectivity information. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications (pp. 107-115). IEEE.

[21] Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classification of RFID attacks. Gen, 15693, 14443.

[22]Deng, J., Han, R., & Mishra, S. (2005). Countermeasures against traffic analysis attacks in wireless sensor networks. In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) . IEEE. (pp. 113-126).

[23] Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the sybil attack. University of Massachusetts Amherst, Amherst, MA, 7.

[24] Fong, P. W. (2011). Preventing Sybil attacks by privilege attenuation: A design principle for social network systems. In 2011 IEEE Symposium on Security and Privacy (pp. 263-278). IEEE.

[25] Margolin, N. B., & Levine, B. N. (2007). Informant: Detecting sybils using incentives. In International Conference on Financial Cryptography and Data Security .Springer Berlin Heidelberg. (pp. 192-207).

[26] Tangpong, A. (2010). Managing Sybil Identities in Distributed Networks. (Doctoral dissertation, The Pennsylvania State University).

[27] Balachandran, N., & Sanyal, S. (2012). A review of techniques to mitigate sybil attacks. arXiv preprint arXiv:1207.2617.

[28] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268).