PRIVACY AND SECURITY CHALLENGES IN IOT APPLICATIONS

Abstract

The Internet of Things (IoT) is becoming an increasingly vital part of modern culture. New technologies like IoT have an impact on the world today. This has resulted in our being encircled by an abundance of technological marvels. These high-tech gadgets simplify and expedite our daily lives. However, we are vulnerable to a wide variety of dangers and cyberattacks. Our personal information is always at risk. There will be several security and privacy concerns due to the widespread nature of IoT technologies. To guarantee precise and accurate confidentiality, integrity, authentication, and access control, among others, IoT requires security and privacy solutions that are credible, inexpensive, efficient, and effective. In this study, we explore the varied uses of IoT and the associated security risks along with potential future research directions for securing and protecting the Internet of Things.

Keywords— Internet-of-Things (IoT), IoT applications, privacy, security

Authors

M. Venkata Krishna Reddy
Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology (A), Hyderabad, Telangana, India
krishnareddy_cse@cbit.ac.in

G. Mamatha
Department of Computer Engineering and Technology
Chaitanya Bharathi Institute of Technology (A), Hyderabad, Telangana, India
gmamatha_cet@cbit.ac.in

Dr. L. Raghavender Raju
Department of Computer Science and Engineering
Matrusri Engineering College, Hyderabad, Telangana, India
lraghavendarraju@matrusri.edu.in

D. Naga Jyothi
Department of Artificial Intelligence and Machine Learning
Chaitanya Bharathi Institute of Technology (A), Hyderabad, Telangana, India
dnagajyothi_cseaiml@cbit.ac.in

Dr. E. Padmalatha
Department of Computer Science and Engineering Chaitanya Bharathi Institute of Technology (A),Hyderabad, Telangana, India
epadmalatha_cse@cbit.ac.in

I. INTRODUCTION

The term "Internet of Things" (IoT) refers to a broad idea that includes many kinds of connected devices and means of communication. The goal of the initiative known as Next Generation Internet (NGI) is to ensure that the development of advanced network infrastructures and to make full use of the opportunities presented by the connection to the physical world, also known as the Internet of Things (IoT). This will be accomplished by utilising advanced computing capabilities and data infrastructure.

There will be billions of people, devices, and services all connected and sharing data and information with one another in the IoT environment overall. These intelligent devices can be used in a wide variety of contexts. Smart environments and self-aware/autonomous devices are the primary goal of the Internet of Things [1, 2]. This includes areas such as smart transportation, smart products, smart cities, smart health, and smart living. Statista [3] predicts that by 2025, there will be 75.44 billion connected devices in use across the globe, up from 20.35 billion in 2017. In the future years, many specific markets should expand by double digits. Consumer electronics, the automobile industry, healthcare, and intelligent buildings and utilities are some of the most promising vertical application fields. Multiple security and privacy concerns have been raised in light of the meteoric rise in the use of IoT applications. As more and more devices get interconnected, this problem will only worsen as new vulnerabilities in security are actually exposed every day. With the proliferation of Internet of Things (IoT) apps and devices, cyberattacks will evolve to become even more sophisticated and dangerous.

For instance, remote attackers might damage implantable medical devices [4] or smart vehicles [5], which could result in substantial financial losses and even put lives at risk. In addition, as IoT devices become more commonplace in government, industry, and the military, criminals have a greater opportunity to compromise national and public safety. Another example is the severe damage done to Iran's nuclear programme by the malicious computer worm Stuxnet [6], which specifically targeted industrial computer systems. However, most businesses and individuals do not understand the importance of privacy and security. The finite usage and resources of IoT devices, however, prevent them from running full-fledged security systems. Consequently, vulnerabilities (such as default passwords or unpatched issues) in IoT devices typically go unpatched for a long time. As the number of exploits, attacks, and data leaks in the Internet of Things (IoT) grows, manufacturers, cloud providers, and researchers are scrambling to design security systems and protocols [7], investigate new vulnerabilities [8], and find efficient means of keeping user information secure [9].

Although academics keep working on protecting the privacy and security of the internet of things (IoT), most of their studies are still in their early phases and lack practicality. There are still many unanswered questions. Threats and failures in the IoT due to a lack of proper security measures could potentially negate whatever advantages it may have. Traditional cryptography systems, security protocols, and protection measures are unavailable or insufficient due to scalability considerations and other limits on device capabilities. It is a significant challenge to ensure that the security architecture is built to last for the expected lifetime of the system (>20 years) and to implement a robust security baseline. It's also reasonable to expect some devices to be compromised when working with a huge device population. Since the Internet of Things (IoT) has specific security, privacy, and

dependability requirements, new approaches and technologies need to be developed to fulfil these needs [10]. The well-being of humanity can be improved by this study of IoT security and privacy because it allows IoT devices to respond to people's preferences, requirements, wishes, and desires without being given specific instructions. These tools benefit society in many other ways as well, including in medicine, meteorology, wildlife identification, and vehicle monitoring. Understanding the privacy and security issues is crucial as IoT becomes an increasingly popular technology due to the proliferation of smart devices. For the sake of humanity, we must learn about and fix these problems. People can help mitigate these Internet of Things (IoT) security and privacy risks. Many surveys have been conducted on the topic of IoT security and published to offer researchers with relevant references and to put researchers in the right path for future study.

II. RELATED WORK

Recent years have seen extensive efforts undertaken to address security and privacy issues associated with the Internet of Things. There have been numerous studies and publications written about the security concerns of the Internet of Things. Current attacks and difficulties were the primary topics of discussion and analysis in Li et al. [11] and Lin et al. [12]. Fu et al. [13] outlined some advantages and disadvantages in two distinct settings: the home and the hospital. Authentication, access control, secrecy, and privacy are only few of the topics that Roman et al. [14] and Sicari et al. [15] covered in their presentations of research difficulties and prospective solutions based on various security techniques. The limitations of IoT devices, such as battery life extension, lightweight computation, classification of security attacks, and control access mechanisms and architecture are just some of the topics covered in the four-part surveys by Weber and Gopi and Rao [16, 17]. Layers of the Internet of Things architecture (including presentation, network, transport, and application) are also discussed. IoT architecture, as described by Chen and colleagues, can be broken down into three main parts: the perception layer, which assumes information collection; the network layer, which handles data transmission; and the application layer, which facilitates recognition and perception between objects and objects, as well as between people and objects, and carries out intelligence-related tasks. The current survey, released by Yang et al. [18], presents the classification of IoT threats and summarizes the major point of earlier surveys. Although these studies addressed most areas of IoT security research, dangers, and open concerns and gave some recommendations for future research, few expose the sources of research difficulties and security risks and clearly define what new challenges emerging from IoT. Another survey of security issues in IoT devices was presented by Tewari and Gupta. This article examines the layered structure of IoT devices and identifies emerging security concerns. Tools and approaches for IoT research were presented, and they highlighted issues related to cross-layer heterogeneous integration [19].

Noor and Hassan, in their 2019 review, compared several studies across several dimensions (including simulation tools, procedures, Internet of Things device security, and personal data protection). It investigates the existing techniques for securing the Internet of Things [20], including authentication, security encryption, trust management, and new technologies. In addition, the unique challenges posed by the protection of private information in the Internet of Things are outlined in a study. Information from experts in the Internet of Things (IoT) who have tried to grasp security and confidentiality issues and have developed new security protocols for effective security and privacy mechanisms (SPMs) [21] is included. There are serious dangers and hacking possibilities associated with almost any

linked gadget. Several levels of architecture, from the field data collecting layer at the bottom to an application layer at the top, are the backbone of the Internet of Things, as demonstrated by Sen [22]. This type of layered architecture needs to be crafted such that it can accommodate the needs of a wide range of sectors, businesses, communities, organizations, and governments. The transport layer of the Internet is responsible for carrying information, the gateway layer and the edge layer help collect information, and the application layer is in charge of how that information is put to use. Sengupta et al. perform an additional investigation into the problems associated with the industrial IoT. A block chain-based solution is explained and categorized based on the destruction of security and privacy attacks [23]. Additional discussions of block chain technology and its characteristics, including access management, decentralization, asymmetric encryption, and smart contracts, can be found in the works of Wang et al. and Weber [24, 25]. This study helps to address that void by discussing and analyzing IoT security challenges from a novel angle: IoT capabilities. The term "IoT features" is used to describe the characteristics of IoT devices, networks, and apps that set them apart from traditional computing devices like smartphones and computers.

III. APPLICATIONS OF IOT

The Internet of Things permeates virtually every facet of our everyday life, including the following categories:

1. **Medical and Health Care System**It's a bright spot for the Internet of Things. Medical equipment can send the patient's critical parameters to a platform, such as a secure cloud, for storage and analysis. The elderly and those with long-term illnesses can receive specialized attention.

2. **Personal and Social Purpose** The applications in this group facilitate communication between users and their immediate environments (such as the workplace or the home) or between users themselves [26].

3. **Environmental Monitoring:** Sensors are used to monitor environmental conditions including air and water quality to ensure their safety. Wildlife habitats are also mapped out through observation. The data collected is utilized to find innovative solutions to environmental problems.

4. **Home Automation :** An automated system can report gas, water and electricity usage to the appropriate utility provider. This method has the potential to better utilize available means. Appliances like the washer, air conditioner, windows, doors, lighting, and fridge may all be optimized through the home automation procedure.

5. **Transportaion:** With the help of powerful computers, actuators, and sensors, both vehicles and roads are playing an increasingly essential role in gathering crucial data for traffic control and guidance [27, 28]. Some of the most prominent transport IoT applications are the Traffic Information Grid (TIG) [29] and the Intelligent Traffic Information Service (ITIS) [30].

6. **Manufacturing** : Manufacturing may be optimised in real time. Sensors and control systems provide for management of production and supply. New items can be made quickly as a result of this.

7. **Services** :From farming and breeding to recycling and environmental management services and energy administration, this field often addresses the conservation, monitoring, and development of all natural resources.

IV. IOT APPLICATIONS IN AGRICULTURE

The following are some of the most important uses of IoT in farming:

- Ploughing, weeding, preparing the seedbed, and planting are all pre-harvest tasks that could be handled by a smart soil cultivation system.
- The artificial supply of water necessary for plant growth might be fully automated with the help of smart irrigation systems.
- In smart fertilizer systems, the quality, quantity, and timing of fertilizer sprayed on the field are all controlled by the system itself.
- The Pest monitoring and Control System monitors and identifies pest infestation, assesses damage to crops, and contains ways for controlling the infestation. - Smart pest detection and control systems.
- Use of smart technologies in livestock breeding and the application of precision agriculture techniques to boost both crop quality and yield constitute "smart livestock farming."
- In order to efficiently gather a field's harvest, a "smart harvesting system" employs Internet of Things-based approaches.
- The goal of a smart farm management system is to enhance farm output through the application of data analytics.
- An intelligent method for managing ground water quality is necessary since the quantity and quality of ground water have a significant impact on the quality of the harvest. Therefore, in this system, procedures are applied using IoT to maintain adequate ground water levels.

V. SECURITY THREATS AND CHALLENGES IN IOT

Human privacy, business process secrecy, and trust in external parties are the three main problems with the Internet of Things. People, things, software, and hardware are all understood to be interconnected, interacting parts of the IoT ecosystem that exchange data through open, untrusted networks. These will inevitably face issues of open trust, privacy, and security.

1. **Security and Privacy Challenges in the IoTs:** Many different types of devices and services are interconnected and share data in the Internet of Things. Security, privacy, and trust norms might vary between zones. There are various security and privacy obstacles that must be surmounted before low-cost, widely accessible IoT devices and services can be established. To name a few of the difficulties:

- **Privacy and Protection:** Because of the pervasive nature of the IoT ecosystem, privacy is a critical component of IoT security. User privacy is a touchy subject in many studies because of the prevalence of online communication and data sharing [31]. Although many studies have been proposed on the subject of privacy, there is still much to learn. Concerns about data security, data sharing, and data management are all yet unanswered research questions [32].

- **Trust Management:** Establishing trustworthy connections between devices is crucial for ensuring their safe interaction in a complex IoT ecosystem. Trust in the interactions between entities and user trust in the system are both important in the Internet of Things [15]. An efficient mechanism for defining trust in a dynamic and collaborative IoT setting is necessary to earn users' confidence. Third, the development of applications based on node trust (such as routing, data aggregation, etc.) [32] are the main objectives of trust research in the IoT framework. Trust management practices should be considered at the conceptual stage of new models designed for decentralized trust environments.

- **Interoperability:** The term "interoperability" refers to the capacity for two or more systems to share and make use of modified data. In order to develop an IoT, a variety of heterogeneous devices, networks, and systems will need to be compatible with one another, making interoperability a crucial component.

- **End Point Security :**It is equally crucial to ensure endpoint security between IoT devices and Internet hosts. For constrained IoT resources, merely applying cryptographic algorithms to packets for encryption and authentication codes is insufficient. Complete end-to-end security requires the safe implementation of protocols for dynamically negotiating session keys (like TLS and IPsec) and algorithms (like AES and Hash algorithms), as well as the verification of individual identity on both ends. End-to-end security in IoT ensures that no third party can eavesdrop on or alter data while it is in transit, giving users peace of mind. Many useful applications rely on correct and comprehensive end-to-end security.

- **Attacks :** The internet of things includes a wide variety of devices that each have their own unique set of capabilities, including memory capacity and processing power. Since these gadgets can be attacked, there needs to be lightweight, impenetrable security options. Devices should have mitigation plans to fend off external threats including denial-of-service and flood attacks. Classification of various IoT security attacks are demonstrated in the figure 1.

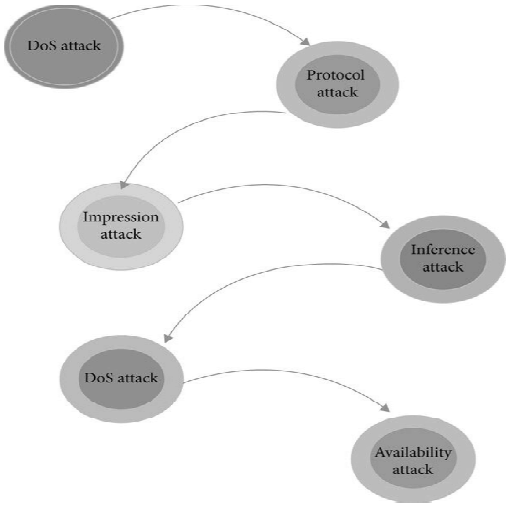

Figure 1: Classification of IoT attacks

2. **Examples of Threats to IoT Security :** Some of the examples are :

- A compromised IoT gadget cab be used as a stepping stone to get access to other, more important gadgets in the network. However, most security technologies lack the visibility into east-west network traffic in real time, rendering these dangers "invisible" for extended periods of time. Many of the most severe cyberattacks can be traced back to this one cause.

- Make use of a vulnerable Internet of Things (IoT) gadget to launch a wider attack across the network. Verizon, in its 2017 Data Breach Digest report, cited the case of a large university that was attacked by a botnet made up of more than 5,000 connected devices, almost all of which were located on the university's network.

- Disrupt the network as a whole by attacking individual systems. As another recent example in Finland, in an apartment block, hackers were able to breach an HVAC controller and turn off many systems.

- Disrupt the machines and make them more destructive. Hackers with access to hospital networks may be able to reprogram pacemakers and insulin pumps that are part of the Internet of Medical Things (IoMT). The fact that these damaged IoMT devices potentially threaten the safety and wellbeing of patients makes this scenario all the more frightening.

- Hackers may breach Internet of Things (IoT) devices and then use them against your business, either by compromising other IoT devices or by stealing data.

VI. SECURITY REQUIREMENTS

Technologies and machines are developing at a rapid rate. Expanding technological capabilities introduce new risks and compromises in personal security. In a shared network, the smart gadgets can talk to one another and share information. If even one device is

compromised, the entire network is at risk. The Internet of Things (IoT) has emerged as a key component of the future Internet, poised to have far-reaching effects on everyday living and commercial settings. More and more IoT apps and services are susceptible to cybercrime and data loss. There are a number of major security concerns, including the four most pressing issues in IoT security are authentication, privacy, availability and data integrity [33]. Figure 2 depicts the security requirements in IoT.

1. **Data Integrity :** The reliability of the information exchanged between two nodes is crucial. Therefore, it is essential that data accuracy be preserved. The exchange of public and private keys via the node requires authentication before a connection can be made between two devices and data theft may be prevented. In a manufacturing company, for instance, if a hacker issues orders to stop production, this is a major problem.

2. **Data Privacy:** The information passed between nodes must be kept secret. The only people who should have access to the information are the sender and the recipient. Protecting the privacy of the information stored within an Internet of Things device is essential. Damage to roads and bridges, as well as potential security breaches, are just two examples of what may happen when hackers gain access to sensitive information stored in the infrastructure sector.

3. **Veracity of Information :** Authentication guarantees that the information you have received is genuine and reliable. By checking that the information received at the destination node has not been tampered with in transit, data integrity safeguards against the practice of "man in the middle" attacks. In the healthcare system, for instance, a patient's information is shared between hospitals. A hacker's tampering with this information could put the patient's care in jeopardy.

4. **Obtainability of Information** Data accessibility is always a top priority in the Internet of Things. It's a major problem if the user can't get to the information. It needs to be fixed immediately. IoT security challenges were examined by Vermesan and Friess [34], who outlined the following needs for a security and privacy framework:

    - Consistent with the resource constrained nature of many IoT devices, lightweight key management solutions are required to facilitate the development of trust relationships and the distribution of encryption materials with little communication and processing resources.
    - Resource-constrained devices supported by lightweight and symmetric solutions.
    - Data identification, authentication, and anonymity are just few of the "Privacy by Design" ideas that can be bolstered with the right tools.
    - Preventing the inference of private information about persons' locations and identities through the observation of IoT-related interactions.
    - Cryptographic methods that allow for the secure storage, processing, and dissemination of data without exposing its contents to unauthorized persons.
    - Using distributed computing and key management to keep data close to home.

Figure 2: IOT Security Requirements

VII. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

Many results on IoT security and privacy indicate that much investigation is required to bring the IoT paradigm to fruition. Suggestions for new lines of inquiry are offered here.

- Since IoT not only handles massive amounts of sensitive data (personal data, commercial data, etc.), but also has the ability to alter the physical world through its control abilities, security and privacy issues must be taken extremely carefully. As a result, cyber-physical environments require security against all threats.
- IoT technologies, devices, and services that will propel IoT growth and bolster IoT vision must be identified, categorized, and prioritized.
- In order to serve the greatest number of people, software, smart objects, or devices, the design of architecture standards should include well-defined abstract data models, interfaces, and protocols, as well as concrete bindings to neutral technologies.
- Creating global directory lookup and discovery services for IoT applications using different identifier schemes; Managing identities; Encrypting/encrypting identities; Authenticating users; Developing new frameworks for global ID schemes.

VIII. CONCLUSION

The primary objective of this article was to present a comprehensive overview of the most critical facets of the Internet of Things, with an emphasis on the vision and security problems that come along with it. IoT's grand ambition is to enable seamless, ubiquitous, and instantaneous connections between devices, people, and information over any available network and service. Smart transportation, smart objects, smart cities, smart health, smart living, and so on are only a few of the many possible applications of the Internet of Things' goal of creating smart environments and self-conscious/autonomous technology. There are still a lot of problems and obstacles to overcome with the Internet of Things. Security and privacy issues, such as authentication and authorization of entities, are also introduced, along with other challenges like ensuring interoperability and achieving a business model in which hundreds of millions of items can be connected to a network. In the future, we may anticipate improved security for smart devices and tighter privacy rules for IoT connectivity, both of

which will make it easier for people to employ automation to get things done. In order to succeed in the Internet of Things (IoT), it must implement improved privacy, data protection mechanisms, and ethical practices. Addressing security issues will remain a top priority for networking and communication researchers in both the private sector and academic institutions throughout the coming years.

REFERENCES

[1] Envista Forensics. (2015).The Most Hackable Cars on the Road. [Online]. Available: http://www.envistaforensics.com/news/the-mosthackable-cars-on-the-road-1
[2] Wikipedia. 2016 Dyn cyberattack. [Online]. Available: https: //en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=76 3071700
[3] The Statistics Portal. (2017). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: https: //www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/
[4] Bigthink Edge. (2016). Hacking the Human Heart [Online]. Available: http://bigthink.com/future-crimes/hacking-the-human-heart
[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” IEEE Internet Things J., vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[6] Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy 9.3(2011):49-51.
[7] CH Kim, T Kim, H Choi, Z Gu, B Lee, X Zhang, D Xu,"Securing Real-Time Microcontroller Systems through Customized Memory View Switching." Network and Distributed System Security Symposium, 2018.
[8] DD Chen, M Woo, D Brumley, M Egele, "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware." Network and Distributed System Security Symposium. 2016.
[9] Le Guan, Jun Xu, Shuai Wang, Xinyu Xing, Lin Lin, Heqing Huang, Peng Liu and Wenke Lee, “From Physical to Cyber: Escalating Protection for Personalized Auto Insurance,” in Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems, SenSys ’16, pp. 42-55, 2016.
[10] Chan, Ellick M., P. E. Lam, and J. C. Mitchell. "Understanding the challenges with medical data segmentation for privacy." Usenix Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies. USENIX Association, 2013, pp. 2-2.
[11] Li, Shancang, T. Tryfonas, and H. Li. "The Internet of Things: a security point of view." Internet Research 26.2(2016):337-359.
[12] J Lin, W Yu, N Zhang, X Yang, H Zhang, W Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications."IEEE Internet of Things Journal., vol. 99, p1 2017.
[13] K Fu, T Kohno, D Lopresti, E Mynatt, K Nahrstedt, S Patel, D Richardson, B Zorn (2017), Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things. Technical Report. Computing Community Consortium. [Online]. Available: http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Securityand-Privacy-Threats-in-IoT.pdf
[14] 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.
[15] S Sicari, A Rizzardi, LA Grieco, A Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks the International Journal of Computer & Telecommunications Networking 76.C (2015):146-164
[16] R. H. Weber, “Internet of things: privacy issues revisited,” Computer Law and Security Review, vol. 31, no. 5, pp. 618– 627, 2015.
[17] A. Gopi and M. K. Rao, “Survey of privacy and security issues in IoT,” International Journal of Engineering & Technology, vol. 7, no. 2.7, p. 293, 2018.
[18] Y Yang, L Wu, G Yin, L Li, H Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things." IEEE Internet of Things Journal 4.5(2017):1250- 1258.
[19] A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.
[20] M. B. M. Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: a survey,” Computer Networks, vol. 148, pp. 283–294, 2019

[21] O. O. Bamasag and K. Youcef-Toumi, “Towards continuous authentication in Internet of Things based on secret sharing scheme,” in Proceedings of the WESS’15: Workshop on Embedded Systems Security, pp. 1–8, Amsterdam, Netherlands, 2015.
[22] 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.
[23] J. Sengupta, S. Ruj, and S. Das Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT,” Journal of Network and Computer Applications, vol. 149, article 102481, 2020.
[24] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, “Blockchain for the IoT and industrial IoT: a review,” Internet of Things, vol. 10, article 100081, 2019.
[25] R. H. Weber, “Internet of Things – new security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.
[26] 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
[27] O. Arias, K. Ly, and Y. Jin, “Security and privacy in IoT era,” in Smart Sensors at the IoT Frontier. Berlin, Germany: Springer, 2017, pp. 351–378.
[28] Gil, D., Ferrández, A., Mora-Mora, H., & Peral, J., "Internet of things: A review of surveys based on context aware intelligent services." *Sensors* 16.7 (2016): 1069.
[29] M. Li, M.-Y. Wu, Y. Li, J. Cao, L. Huang, Q. Deng, X. Lin, C. Jiang, W. Tong, Y. Gui et al., “Shanghaigrid as an information service grid: An overview,” in Services Computing, 2005 IEEE International Conference on, vol. 1. IEEE, 2005, pp. 351–354.
[30] X. Li, J. Wu, X. Lin, Y. Li, and M. Li, “Itis: Intelligent traffic information service in shanghaigrid,” in ChinaGrid Annual Conference, 2008. ChinaGrid’08. The Third. IEEE, 2008, pp. 10–14.
[31] M. Langheinrich, “Privacy by designprinciples of privacy-aware ubiquitous systems,” in Ubicomp 2001: Ubiquitous Computing. Springer, 2001, pp. 273–291.
[32] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, “A systemic approach for iot security,” in Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE, 2013, pp. 351–355.
[33] J. Lopez, R. Roman, and C. Alcaraz, “Analysis of security threats, requirements,technologies and standards in wireless sensor networks,” in Foundations of Security Analysis and Design V. Springer, 2009, pp. 289–338
[34] O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, 2013.

