IoT Security: A Brief Review

Moni sree H [1], Nithyaa Shri R B [2], Pavithra R [3], Sasikala S[4]
[1][2][3][4] Department of Electronics and Communication Engineering
Kumaraguru College of Technology
Coimbatore, India
monisree.18ec@kct.ac.in, nithyaashri.18ec@kct.ac.in, pavithra.18ec@kct.ac.in, sasikala.s.ece@kct.ac.in

Abstract—**The Internet of Things (IoT) is the rapidly developing technology that facilitates communication between devices in a network for collecting, processing, and exchanging data. This enables controlling and accessing the devices remotely. IoT figures a great advancement in almost all the fields as it finds application in various sectors like medical applications - Healthcare, Industrial applications – IIoT, smart city applications, environmental applications, consumer IoT and so on. When several devices are connected in a wide network where each device data is accessible by other devices in the same network. In such a case, data security hits the highest priority while designing an IoT system. This paper deals with a detailed survey on the architecture of IoT systems, security parameters of IoT systems security, security in various blocks of IoT systems, and the critical security applications in the areas of IoT.**

Keywords: Internet of Things, consumer IoT, IIOT, healthcare, critical security.

I. INTRODUCTION

IoT products are widely being implemented and allowing the development of new applications, with surveys predicting that there will be over 20 billion Internet of Things (IoT) devices by 2030 [1] and estimated global market size of $457 billion by 2030 [2]. These solutions cover a wide range of situations, from smart homes to smart manufacturing processes in the industry. IoT technologies should be secure by design to achieve such a degree of diffusion and control, as well as due to the close coupling with the physical realm [3]. This means that protection should be considered a key system-level property and factored into the actual design of IoT solutions architectures and approaches [4].

In recent years, we've seen an increase in attacks ranging from individual-targeted attacks, such as those triggered by IoT botnets, to nationwide attacks, such as those triggered by video baby monitors inside home automation [5]. While these cyber-attacks have helped to raise IoT risk awareness, vulnerable devices continue to be released into the market, resulting in privacy breaches, financial costs, and even death. Part of the issue is that manufacturers hurry to release revolutionary products that appeal to customers and gain a head start on the competition, but fail to protect a key functional necessity. Another reason is that many manufacturers in the IoT domain are dissatisfied with protection [6].

Main IOT Security includes [7],

- IoT devices need to be carefully provisioned with security measures.
- IoT systems are composed of devices having limitations in terms of their software and hardware.
- Only lightweight algorithms are preferred for security.
- IoT with heterogeneous technology produces a large amount of heterogeneous data increasing the attack surfaces.

The concept of IoT lies in internetworking of physical devices so that every device gets connected with the other devices without the intervention of the user or with minimal intervention of the user. Wherever we deal with processing data, security seems to be the first concern to avoid the disclosure of user's data.

The main goal of this paper is to emphasize the Architecture and layers used that for IoT security, primary needs for security, security parameters, Various levels of security for high-end devices, and Critical applications facing security issues using IoT taxonomy.

II. ARCHITECTURE OF IOT SECURITY SYSTEM

The research on IoT security architecture and its key technology [8] provides a clear-cut idea about the various layers of IoT systems based on their characteristics. It provides aresearch analysis on the classification of IoT systems into a four-layer model which builds a scientific and rational architecture for IoT systems. The IoT security architecture has four layers namely perceptual layer, network layer, processing, and application layer [8] which is classified based on the three main characteristics: Comprehensive perception to obtain proximity of the devices at anytime and anywhere, reliable transmission for accurate delivery of data between various devices in a network and intelligent processing to process massive data. [8]

III. ANALYSIS OF ARCHITECTURE AND THE VARIOUS LAYERS

The perceptual layer realizes the comprehensive perception of information [8]. This incorporates the information security at the level of collecting the data from sensors, RFID, GPS, any other input devices are to be secured. For this, a regular safety inspection, authentication, and secured transmission between sensor nodes are to be assured [8].

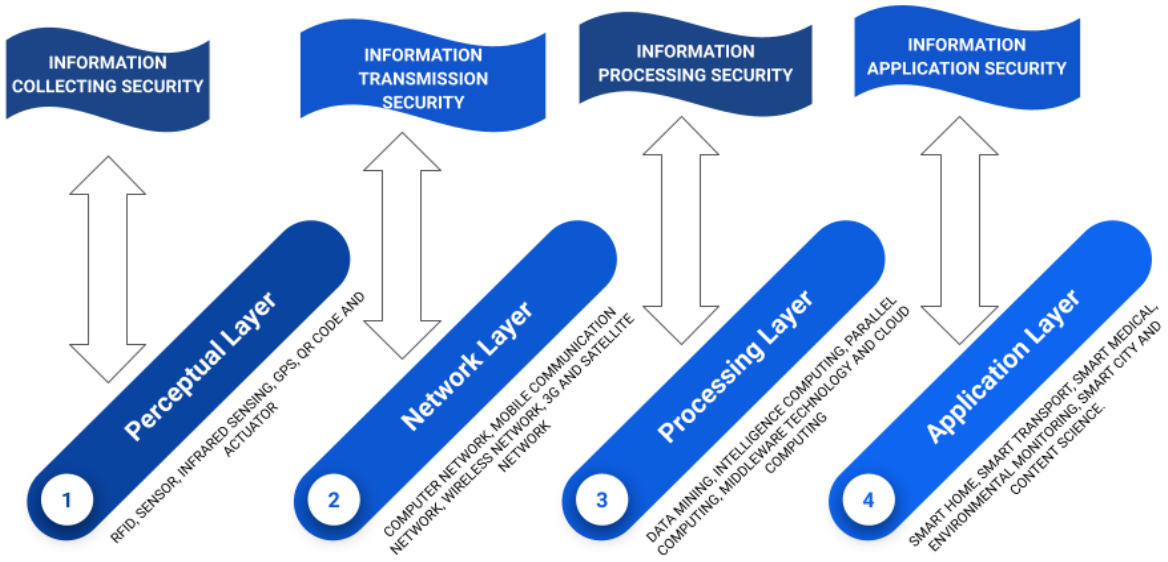

Figure 1: Security Layers

Next is the network layer which realizes the reliabletransmission of information through various transmission techniques such as long-distance cable communication, wireless communication, and network communication [8]. When this transmission occurs network layer can be corrupted by fake routing information, selective forwarding/non-forwarding, and black hole attacks. The processing layer realizes the intelligent processing of information based on data mining and cloud computing technologies to process massive data [8]. This enables intelligent decision-making and control and also ensures interoperability and scalability. The processed data reaches the application layer which realizes the authorization management to strengthen the data information as the cloud computing processes a large amount of heterogeneous data [8].

IV. Security needs of IoT systems and the primary technologies involved

To maintain the security of systems: security, confidentiality, validity, and integrity of data information should be guaranteed to ensure information collection, information transmission, and information processing and information application security an outline of various security policies is provided [9].

Physical hardware security policy[8] involves the security of information collection at the sensor level. For this RFID technology which is used to store information on specification and interoperability and its security policy is mentioned. The asymmetric key cryptographic method has 2 keys to prevent the leakage of information due to hackers, a man-in-middle attack.

Wireless sensor network security[8] *policy* realizes the cooperatively collecting, processing information of the perceptual objects in the network. To establish sensor security at network levels integrated security policies are employed wherein the idea of multipath routing policy improves the security of the entire network with prevention of DOS, congestion, and node replication attacks.

Information collection security policy[8] realizes the authentication strategy used for preventing malicious users to access the database, further securerouting strategies and symmetric/asymmetric strategies used to strengthen perceptual layer information preventing attacks like eavesdropping, tampering, and replay attacks which are information collection attacks.

Finally, the *information transmission*[8] *and processing policy realize* data confidentiality and authenticity to prevent security risks such as denial of service attacks, a man-in-the-middle attack, unauthorized access. So, to ensure data security at this level various techniques like authentication, filtering, and detection mechanisms are employed.

V. Security parameters of IoT systems

To attain maximum level of security at each layer and levels of communication some security principles are to be followed to prevent serious hack attacks and also to prevent inevitable access of user's personal information [9]. Those parameters are discussed in the system testing methodology of IoT.

Confidentiality: In a wide network wherein, each node is connected to the other has a high chance of leakage of information to various other nodes. In that case authorization of data and the data management issues are to be addressed

to maintain the confidentiality of data without leaking it to unauthorized nodes [9].

Integrity: To ensure the precision of data from the right sender in communication between various interconnected devices integrity plays a vital role. This can be achieved by ensuring end – end security of communication by imposing firewalls and other encryption techniques [9].

Availability: Various devices getting connected at the same time and accessible at any time is the primary aim of IoT. So, to ensure the data availability and the availability of devices that provide essential data in the IoT network is realized in this principle[9].

Authentication: In a large network with a large number of entities the identification and authentication seem to be challenging when there is manual intervention. It should be accurately done before disclosing information as they do not know each other (at the initial time)[9].

Lightweight systems and Heterogeneity: A single IoT network involves different kinds of devices and different communications are performed between various entities. This marks the heterogeneous system which connects various heterogeneous things. So the system should be designed in such a way that it gets connected to all devices at any time. So to guarantee security in such a dynamic environment an accurate encryption system is required with optimum security protocols[9].

*Policies and key management systems:*To ensure efficient data management, protection, and transmission in a dynamic IoT environment with various heterogeneous components, the establishment of policies leads to growth and scalability of IoT, developing trust in humans to use IoT devices. Encryption algorithms play a vital role in security in particular in the integrity of IoT systems. To ensure confidentiality in data between smart devices encryption keys are used for lightweight key management systems enabling trust between them [10].

VI. Security in IoT at various architecture levels

*Communication security in IoT:*To exchange the information between the users/devices we need security. Authentication [11] and access control are the security features and are privacy problems in networking. If we want to make information private without the nonexistence of a third party, mutual authentication is necessary for IoT devices[12]. Both the data receiver and data transmitter need to verify the data in the heterogeneity of the IoT environment. Authentication key establishment protocol, we need to establish the key while transferring the information, so that we can maintain our security. Access control[13] will ensure the new connection and establishes the quality of communication.

Security in end applications: To transmit a huge amount of data to a different location over the different networks there is a possibility of losing our privacy such as health care, transportations, smart cities, etc. But in IoT data from the user is sensed and then it is transported with their consent and knowledge. The privacy concern [14] include the fingerprint and heartbeat due to environmental aspects there is a possibility of reducing privacy.

Forensic challenges: When IOT infrastructure is used to carry the information, it will call for forensics' investigation of IoT that will make our information very private. In this, data is sensed and then it will transmit over the data holders[15]. IoT forensics is nothing but it is a combination of network, device, and cloud. The privacy model for IoT is an important model that has been the forensic model [16] for IoT. With the help of the ProFIT model, the information can be gathered by the end devices and it helps in the reconstruction of the scenes to an accurate level.

Application security in IoT:The Internet of changed people's lives in various applications such as health care, smart city, industry, manufacturing, security, and emergencies.

VII. Critical security application in the areas of IoT

Almost all IoT solicitations that have been situated or are in the process of being deployed need a high level of security. IoT technologies are increasingly expanding and infiltrating[17] the majority of existing industries. While existing networking technologies help operators support these IoT applications, many of them need more rigorous protection from the technologies they use. Various hostage-critical IoT solicitations taxonomy are deliberated in this division.

*Cities becoming smart nowadays – **Smart Cities**:*

To improve people's overall quality of life, smart cities make comprehensive use of new computation and connectivity resources [18]. Smart buildings, smart traffic management, smart disaster management, smart infrastructure, and so on are all part of it. Cities are being pushed to become smarter, and governments all over the world are fostering their production through various stimuli [19]. While the use of tingle apps is induced to enhance citizens' overall quality of life, it also poses a challenge to their solitude. Key card systems tend to place citizens' credit card information and purchasing habits at risk. Nevertheless, if such apps are compromised, the child's protection could be compromised come to take a chance. User's location traces can be leaked by smart mobility applications. There are apps that parents can use to supervise their children. Nevertheless, if such systems are hacked, the child's protection could be compromised.

*Environment teaches us a lot – **Smart Environment**:*

The taxonomy of the Smart Environment includes Smart animal farming, Smart agriculture, Wild vegetation monitoring, domestic waste treatment monitoring, Regional Climate change monitoring, etc… All of these Internet of

Things technologies are intertwined with the lives of people and animals in those regions. The knowledge from these IoT applications can also be used by government agencies working in these fields. Security flaws and vulnerabilities in any environment involving IoT applications can have disastrous consequences. Similarities can have catastrophic consequences for IoT applications in this sense. For instance, if the solicitations begin wrongly examining seismograph, the government and businesses will experience financial losses. If, for instance, the trenching is unable to anticipate the seismograph, that results in property and life loss. As a result, smart environment implementations must be extremely accurate, and data tampering and security breaches must be avoided. Monitoring soil moisture, controlling microclimate circumstances, selective drenching in dry zones, and controlling wet zones and inversion both are part of smart agriculture. The application of such advanced features in tillage makes farmers achieve high productivity and avoid financial losses. Fungus and other microbial contaminants can be prevented by controlling dryness and wetness levels in various kernel and vegetable production. Controlling the climate can also aid in increasing the production and quality of vegetables and crops. There are many emerging features in this field that help in controlling the activities and health conditions of farm animals by attaching agitator to the animals, comparable to crop keep track of organism's health. If such solicitations are hacked, it may result in the piracy of farm animals, as well as crop damage from adversaries.

Machines are getting smart!! – ***Smart Industries****:*

The main taxonomy of the industrial application includes Smart metering, Smart Grids, Scheduling systems, and many more… Smart metering covers a wide range of applications for various measurements, tracking, and management. Smart grids, where electricity utilization is constant and controlled, seem to be the most common application of smart metering. Smart metering may also be used to combat energy theft [20].Smart meters may also be used to measure the levels of gasoline and important parameters in water tanks and storage tanks Water grids are also available. It is necessary to keep track of and improve the efficiency of solar cells array energy from living organisms by adjusting angle with the sun in a dynamic way solar panels to get the most out of the sun zeal. Smart meters are often used in some IoT applications to calculate the water compulsion in water transport systems or the weight of products. Smart metering devices, on the other hand, are endangered to both physical and cyber-bombard, while traditional meters can only be tampered with physically. Smart meters, also known as advanced metering infrastructure (AMI), are designed to do more than just monitor energy consumption. All electric equipment in a home is connected to smart meters in a smart home area network (HAN), and the data obtained to control all the devices can be used for load and cost control. Intentional violation into such communication structure by a customer or a combatant can alter the information that is maintained and leads to the loss of consumer protection [21].

Commercial Application:

This taxonomy includes Shopping systems and retail. In the retail industry, IoT technologies are widely used. Several solicitations have been created to maintain the storage resources of products that travel across the different chains. Internet of Things has been emerged to control goods in warehouses so that restocking can be achieved as efficiently as possible. Various intelligent shopping apps are now being created to assist consumers to owe their tastes, behaviors, hypersensitivity to certain ingredients, and other factors. The use of the augmented reality that has changed the people's life to their extent. Security concerns have arisen in the deployment and use of various IoT applications by several retail companies [22]. Adversaries can attempt to compromise IoT applications related to goods storage conditions, as well as submit incorrect that gave many ideas about products to users to increase their sales. Customer's privacy details and other personal information can be stolen if security natures have not been in smart retail, resulting in monetary losses for both the customers and retailers.

*General Application –****Smart Home****:*

The trending technologies that have been implemented in IoT technologies are home automation. This contains applications where the people can monitor their equipment remotely and intruder detection systems installed on windows and doors, and so on. Energy and water use are being tracked using monitoring systems, and consumers are being encouraged to save money and resources. Many codes are developed to secure our privacy [23]. Intensions are identified by exchanging the user's behavior in key areas of the house to their usual activity in those areas[24]. Attackers can, however, gain unsophisticated to the Internet of Things devices in the home and attempt to damage users. For example, since the implementation of various home automation systems, the number of home burglaries has risen dramatically [25]. In the past, adversaries have attempted to measure the form and amount of Internet traffic to and from the smart home to assess the residents' actions and presence[25]

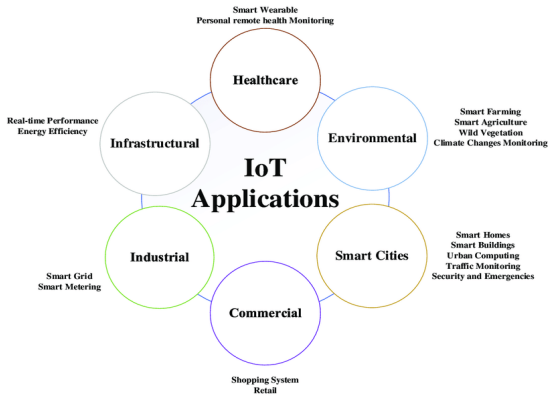

Figure 2: Application Taxonomy

VIII. Conclusion

The main contribution of this paper includes IoT system architecture, principles, and threats that have been occurred in the different layers of IoT architecture. It also focuses on security needs and requirements available in the IoT application. The security testing methods seem to be challenging when applied to real-world applications. The cyber-attacks have incorporated that these security standards and protocols have failed in providing security to the IoT device. Hence to tackle the current security in IoT application we need a novel and worthy IoT security system that should be very protractile and it should help to all the end-users and applications. To overcome these issues ML is an inherent tool that is blended with SDN, to make our privacy in a very secure manner. It can also solve the security issues using their trained Mathematical expression. In the future, by keeping the key of SDN and ML we can protect the IoT system against most security attacks.

References

[1] Gartner Inc., "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," 2018. [Online]. Available: https://www.gartner.com/newsroom/id/3598917.

[2] L. Columbus, "2017 Roundup of Internet Of Things Forecasts," 2017 [Online]. Available: https://goo.gl/MCKCNa.

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

[4] B. Vogel and R. Varshney, "Towards designing open and secure IoT systems," In 8th International Conference on the Internet of Things, pp. 1–6, 2018.

[5] J. Bugeja, D. Jonsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," In IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 537–542, 2018.

[6] Cloud Security Alliance, "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products,". 2016.

[7] 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.

[8]"The Research on IoT Security Architecture and Its Key Technologies", in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2018, pp. 2,3,4.

[9]"Security Testing Methodology of IoT", in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2018, pp. 2,3,4.

[10]D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici, "A survey on secure communication protocols for iot systems," in 2016 International Workshop on Secure Internet of Things (SIoT). IEEE, 2016, pp. 47–62.

[11]H. Kim and E. A. Lee, "Authentication and authorization for the internet of things," IT Professional, vol. 19, no. 5, pp. 27–33, 2017.

[12] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, vol. 31, no. 5, pp. 618–627, 2015.

[13]S. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in 2015 IEEE International Conference on Services Computing. IEEE, 2015, pp. 279–284.

[14]A. Banafa, "Iot standardization and implementation challenges," IEEE Internet of Things Newsletter, 2016.

[15] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the internet of things," in 2016 IEEE Symposium on Computers and Communication (ISCC). IEEE, 2016, pp. 1109–1111

[16] F. I. Khan and S. Hameed, "Software defined security service provisioning framework for internet of things," arXiv preprint arXiv:1711.11133,2017.

[17] I. Farris, J. B. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, ´ A. Skarmeta, and B. Sahlin, "Towards provisioning of sdn/nfv-based security enablers for integrated protection of iot systems," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017, pp. 169–174

[18] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, ''Smart cities: A survey on data management, security, and enabling technologies,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[19] D. Eckhoff and I. Wagner, ''Privacy in the smart city—Applications, technologies, challenges, and solutions,'' IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.

[20] X. Xia, Y. Xiao, and W. Liang, ''ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 445–458, 2019.

[21] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, ''Toward a secure wireless-based home area network for metering in smart grids,'' IEEE Syst. J., vol. 8, no. 2, pp. 509–520, Jun. 2014.

[21] N. N. Dlamini and K. Johnston, ''The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review,'' in Proc. Int. Conf. Adv. Compute. Commun. Eng. (ICACCE), Nov. 2016, pp. 430–436.

[22] A. C. Jose and R. Malekian, ''Improving smart home security: Integrating logical sensing into smart home,'' IEEE Sensors J., vol. 17, no. 13, pp. 4269–4286, Jul. 2017.

[23] I. Tudosa, F. Picariello, E. Balestrieri, L. De Vito and F. Lamonaca, "Hardware Security in IoT era: the Role of Measurements and Instrumentation," 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT), Naples, Italy, 2019, pp. 285-290.

[24] N. M. Karie, N. M. Sahri and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 2020, pp. 22-29.

[25] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil,M. Guizani, and A. Al-Fuqaha, ''Smart cities: A survey on data management, security, and enabling technologies,'' IEEE Commun. Surveys Tuts.,vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[26] E. K. Markakis, K. Karras, N. Zotos, A. Sideris, T. Moysiadis, A. Corsaro,G. Alexiou, C. Skianis, G. Mastorakis, C. X. Mavromoustakis, andE. Pallis, ''EXEGESIS: Extreme edge resource harvesting for a virtualized fog environment,'' IEEE Commun. Mag., vol. 55, no. 7, pp. 173–179,Jul.