International Journal of Recent Development in Computer Technology & Software Applications
http://eurekajournals.com/IJRDCTSA.html
ISSN: 2581-6276

Exploring Security Challenges in the Internet of Things: A Comprehensive Literature Review

D. Lalitha Ashwini[1]

[1]Department of Computer Science, TSWRDC(W), Karimnagar, Telangana, India.

Abstract

The increasing integration of IoT technology into everyday life has become prominent across sectors such as healthcare, banking, and household management. IoT devices serve multifaceted purposes ranging from home safety measures like fire prevention to environmental monitoring. However, amidst these benefits, ensuring the security and privacy of IoT systems is a critical concern.

Due to the heterogeneous nature of IoT devices, encompassing various types, networks, and protocols, a one-size-fits-all approach to security is impractical. Each device type presents unique security challenges that require specific attention. Consequently, there's a need to analyse existing protocols and mechanisms to develop tailored security solutions for different IoT applications.

Conducting a survey of heterogeneous IoT devices and their associated security issues is essential. Such research provides valuable insights into the diverse threats posed by various types of IoT applications, enabling stakeholders to implement targeted security measures.In summary, the discussion around IoT security necessitates a nuanced understanding of the challenges posed by different devices and applications. By conducting thorough research and analysis, stakeholders can develop effective strategies to safeguard IoT ecosystems without compromising on functionality or privacy.

Keywords: Internet of Things, Security, Privacy.

Introduction

The Internet of Things (IoT) is a paradigm that involves connecting devices to the internet and to each other, creating a network where people and objects can communicate and share information [1]. This connectivity facilitates the integration of everyday objects, such as home appliances and surveillance cameras, with microcontrollers and transceivers for digital communication. However, the diverse range of devices connected to IoT introduces the challenge of

heterogeneity, encompassing different types of networks, data, and technologies. Addressing the needs of such a heterogeneous environment presents a significant challenge.

IoT is a convergence of various elements in the digital realm, combining humans, computers, and smart objects to form a cyberspace. Existing network systems, including cloud computing, social networks, industrial networks, and the internet, contribute to this interconnected landscape. The evolution of heterogeneous networks has led to concepts such as the Cloud of Things (CoT), Web of Things (WoT), and Social Internet of Things (SIoT)[2].

Related Work

Numerous research efforts have focused on mitigating the risks associated with physical IoT functions. A survey conducted in this domain reveals four main areas of focus: The initial section addresses the constraints faced by IoT devices, while the subsequent part categorizes attacks. The third segment provides an overview of authentication architectures, and the fourth discusses security concerns across different layers [3].

While IoT applications offer significant benefits to users, concerns about security remain paramount. Despite the willingness of consumers to invest in IoT devices, manufacturers often overlook the importance of robust security measures. The proliferation of internet-connected systems increases the risk of creating insecure environments[4]. Security and privacy are major concerns for consumers, as IoT devices not only collect personal data but also monitor user activities. This necessitates careful consideration before disclosing personal data, whether stored in public or private clouds[5].

Recent surveys indicate that a significant portion of IoT devices have experienced security breaches, resulting in the theft of personal information. Such incidents can lead to a loss of confidence in data security and integrity. A conceptual framework from 2020 defines IoT as a combination of services, data, networks, and sensors, with four key technological enablers driving its implementation[6].

For tagging objects, RFID (Radio Frequency Identification) technology is utilized. To sense objects, sensor technology is employed. Smart technology is utilized for processing and analyzing data from objects. Nanotechnology is employed for miniaturizing objects [7].

The basic architecture of IoT comprises three layers:

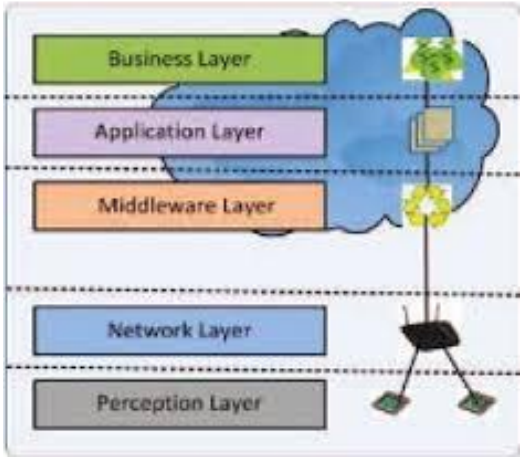
Application Layer: This layer encompasses various applications and services.

Network Layer: It includes network communication software and physical components such as topologies, protocols, and network nodes used in communication.

Perception Layer: This layer consists of different kinds of sensory technologies.

IoT represents a convergence of heterogeneous networks, incorporating chip technology. The rapid expansion of internet applications spans various domains such as agriculture, smart

communities, and control and tracking systems. Research analysis conducted in 2020 suggests that IoT objects will become integrated into human social life [8].



Security is paramount in the rapid advancement of IoT-based applications in today's environment. However, traditional security architectures and standards for IoT often fall short when dealing with the diverse range of intelligent devices in use. The heterogeneity of these devices presents a significant challenge, requiring innovative solutions to ensure robust security measures are in place.

Numerous literature surveys have explored IoT security, categorizing attacks and proposing solutions. Andrea et al.[9] introduced a new classification of IoT device attacks, categorizing them into physical, network, software, and encryption-based attacks.Each layer of the IoT architecture has its own security implications. Physical layer attacks occur when an attacker is in close proximity, while network attacks target the networking components of IoT systems.

Preventive measures include implementing hash and cryptographic algorithms at the physical layer and authentication mechanisms at the network layer. The application layer can enhance security through authentication, encryption, and integrity verification, allowing only authenticated users to execute transactions.

Porambage et al. proposed a pervasive authentication protocol and key establishment scheme, known as Pauth Key, for resource-constrained wireless sensor networks in distributed IoT applications[10]. This protocol involves a registration phase and an authentication phase to register devices and establish keys securely.

Zhang et al.[11] proposed a DDoS attack prevention algorithm involving four nodes: working, monitoring, legitimate user, and attacker. Working nodes collect information, differentiate between genuine and malicious requests, and store legitimate requests for future reference, effectively detecting users upon subsequent requests. This algorithm effectively mitigates DDoS attacks. Bouij et al. introduced SmartOrBAC, an extended authorization access control model supporting the network layer of IoT frameworks. Dividing the IoT network framework into constrained, less constrained, organization, and collaboration layers, SmartOrBAC enhances security features by incorporating Client Authorization Engine (CAE) and Resource

Authorization Engine (RAE), making it user-friendly and error-reducing compared to capability-based models.

Conclusion

This survey paper delves into the architecture of IoT, which comprises various layers. The variations in IoT architecture stem from the diverse array of devices connected to it. Security concerns within IoT applications are thoroughly examined. The level of security of commercially available devices in the market is contingent upon the technologies employed, the protocols implemented, and the specific security mechanisms utilized for individual applications. However, these mechanisms vary from one device to another. By analysing IoT attacks, it's possible to develop generalized techniques applicable to IoT applications.

References

L. Atzori, A. Iera, and G. Morabito, “The internet of things” A survey, Comput. Netw, 2010 , vol. 54, no. 15, pp. 2787-2805.

Ke Xu, Yi Qu, and Kun Yang. “A Tutorial on the Internet of Things:From a Heterogeneous Network Integration Perspective” IEEE network,March/April 2016.

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li_, and Hongbin Zhao “A Survey on Security and Privacy Issues in Internet-of Things”

Margaret Rouse, “Iot security (internet of things security),” Internet of-Things-security, 2013.

J. Granjal, E. Monteiro, and J. S. Silva, “A secure interconnection model for ipv6 enabled wireless sensor networks,” in 2010 IFIP Wireless Days, Oct 2010, pp. 1-6

L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," Ad Hoc Networks, vol. 56, pp. 122-140, 2017.

L. Srivastava and T. Kelly, "The internet of things," International Telecommunication Union, Tech. Rep, vol. 7, 2005.

K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013, pp. 663-667.

I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of things: Security vulnerabilities and challenges,” in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180-187.

P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “Pauthkey: A pervasive authentication protocol and key Establishment scheme for wireless sensor networks in distributed iot applications,” in International Journal of Distributed Sensor Networks, 2014.

C. Zhang and R. Green, “Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network,” in Proceedings of the 18th Symposium on Communications & Networking, ser. CNS ’15. San Diego, CA, USA: Society for Computer Simulation International, 2015, pp. 8-15.