Exploring the evolving landscape of security threats in IoT: Challenges and Countermeasures

Aakash Acharjee, Sabyasachi Mondal, Rishabh Pipalwa, Arjun Mitra, Abhijit Paul

***Abstract*--This paper analyzes the security threats confronting Internet of Things (IoT) devices and systems. The proliferation of connected devices has led to an abundance of data that can be harnessed for diverse purposes. Nonetheless, this increased connectivity and interdependence of IoT systems have also brought forth novel and intricate security threats. These threats carry the potential for severe ramifications, encompassing physical harm, financial losses, and the impairment of critical infrastructure and services. The study delves into the various forms of security threats that IoT systems encounter, encompassing malware, data breaches, and denial-of-service attacks. Furthermore, the paper evaluates the current state of IoT security and contemplates the future of IoT security solutions, considering the potential impact of emerging technologies like AI and ML. A holistic approach to IoT security is advocated, emphasizing collaboration among stakeholders, the adoption of security standards, and the development of secure-by-design IoT devices.**

***Index Terms*--AI; Blockchain; IoT; ML; Threat.**

I. INTRODUCTION

THEInternet of Things (IoT) has revolutionized the way we interact with technology, allowing us to automate and optimize various aspects of our lives. IoT has made it possible for us to control our houses, keep an eye on our health, and increase productivity in sectors like manufacturing and transportation. IoT's rapid use has, however, also brought with it a fresh batch of security risks.

The IoT ecosystem is characterized by the interconnectivity of various devices and systems, ranging from smart home appliances to industrial control systems. As a result, security vulnerabilities in one device can potentially affect the entire network, leading to catastrophic consequences. Moreover, the lack of security standards and regulations has made IoT devices an attractive target for cybercriminals. As more critical infrastructure and services rely on IoT devices, the potential impact of security breaches has become more significant. As per International Data Corporation, there will be approximately 40 billion IoT - connected devices, or "things," in the market by 2025 [1]. It also says that industrial and manufacturing equipment represent the strongest possibility for connected "things," but that smart home and wearable devices will see rapid adoption soon.

The shortage of energy (or power) is the basic need of the population, and it is one of the major problems worldwide. Central power agencies of the Republic of India shared data on power consumption where 6.5TWh is consumed for public lightning and takes the expenditure to $500 million annually [2]. The daily expenditure can have an alternative solution using IoT devices such as installations of solar panels in streetlight arenas. There are multiple IoT protocols such as MQTT which monitor the surrounding environment and adjust light intensities [3-4]. These IoT infrastructures with IoT protocols can conserve a higher amount of energy.

This paper has examined the dynamic realm of security threats in IoT and addressed the obstacles and strategies required to alleviate them. We have presented an extensive evaluation of the existing condition of IoT security to identify crucial areas necessitating enhancement. We have delved into the diverse categories of security threats encountered by IoT systems, encompassing their potential consequences and the factors that contribute to their susceptibility. Additionally, we have scrutinized the present state of IoT security, encompassing the challenges and possibilities involved in implementing robust security measures.

II. SECURITY THREATS

Security threats are classified into two main categories: hardware threats and software threats. Hardware threats involve attacks on physical devices, while software threats include malware that can hijack devices and the interception and modification of data during transit [5].

A. Hardware threats on IoT devices and networks

This document may be used as a template for preparing your Transactions/Journal paper. You may type over sections of the document, cut and paste into it, and/or use markup styles….Hardware-level threats are a common occurrence in IoT devices and networks where standard protocols are absent. Due to the limitations of many small IoT devices, generic protocols are designed with a default level of security, as heavyweight protocols are impractical. Consequently, IoT protocols often prioritize smooth and efficient operations over robust security measures. As a result, both IoT devices and

A. Acharjee,Department of Information Technology, Amity University, Kolkata, India (e-mail: aakashacharjee0@gmail.com).
S. Mondal, Department of Mathematics, North-Eastern Hill University, Shillong, Meghalaya, India (e-mail: sabya.mondal.2007@gmail.com).
R. Pipalwa, Department of Information Technology, Amity University, Kolkata, India (e-mail: rishabhpipalwa@gmail.com).
A. Mitra, Department of Information Technology, Amity University, Kolkata, India (e-mail: arjung0055@gmail.com).
A. Paul. (Corresponding Author), Department of Information Technology, Amity University, Kolkata, India (e-mail: a_paul84@rediffmail.com).

Volume 2, Issue 2
https:// doi.org/10.15864/ajac.22013

networks are highly vulnerable to various threats, including hardware trojans, side-channel attacks, tampering, Denial of Service (DoS), and Distributed DoS (DDoS).

Hardware trojans involve an attacker monitoring, modifying, or disabling data stored in devices [6-7]. These trojans gain control and activate their strategies within the devices or networks. Strategies are implemented either sequentially, based on specific sequences, or combinational, triggered by certain conditions. Side-channel attacks occur when attackers exploit the physical disclosure of information from running devices. Attackers continuously monitor device characteristics such as power consumption, electromagnetic emissions, and time-related information. When an opportunity arises, they attack the non-invasive hardware components of the device to extract sensitive information like encryption keys or passwords. Techniques used in side-channel attacks include differential error analysis [8], performance monitoring attacks [9], acoustic decryption key extraction attacks [10], and electromagnetic analysis attacks [11].

Tampering is another threat that arises when attackers modify existing data on IoT devices. In many IoT environments, there are no physical safeguards to prevent attackers from gaining access. Consequently, attackers can physically interact with the device or exploit vulnerabilities in the software to tamper with the data by compromising the device's firmware. Attackers may also install malicious software during this phase, altering the device's behaviour. DoS and DDoS attacks involve attackers interfering with the internal workings of the device, thereby denying authorized users access to services.

B. Software threats on IoT devices and networks

Similar to hardware threats, software threats pose a significant risk to the security and functionality of IoT devices and networks. These threats can compromise the protection of stored data and disrupt the provision of services to subscribers. Common software-level attacks include Botnet, Spoofing, and DoS.

In a Botnet attack, malware-infected devices are connected to the Internet. As IoT devices often lack robust security solutions due to their limited resources, they become easy targets for attackers. By converting these compromised devices into a botnet, attackers gain complete control over them. Botnets are then utilized to carry out various malicious activities such as phishing attacks, spam distribution, malware delivery, and DDoS attacks. Botnet architectures can take the form of peer-to-peer, client-server, or a combination of both [12].

Spoofing occurs when attackers impersonate valid IoT devices or authenticated users to acquire control to the network. These attacks involves acquiring the MAC or IP address of legitimate users to deceive the network.

Similarly, to its impact on hardware, DoS attacks can also target the software components of IoT devices. Attackers often employ their own devices to flood a target with an overwhelming number of messages or data, resulting in a DoS condition. Once a DoS attack occurs, even though the server is operational, authenticated, or legitimate subscribers are unable to access the services they require. Attackers intentionally flood the network with excessive data to create congestion or blockage in the communication path between the service provider and the subscribers. Common types of DoS attacks include UDP floods, ICMP floods, Ping floods, and more [13-14].

III. SOLUTIONS TO IOT SECURITY THREATS

The conventional approach to addressing hardware and software threats in IoT devices and networks revolves around protecting data. Data protection encompasses safeguarding data at rest, which is stored on the device, as well as during transmission and reception, known as data in transit. Various methods can be employed to protect data and prevent attacks.

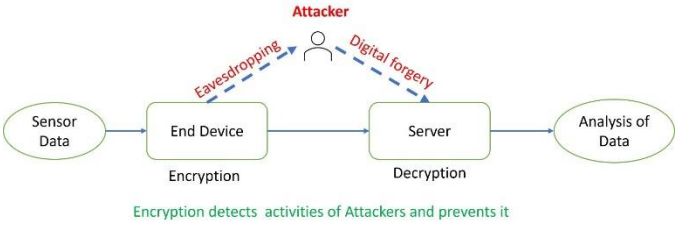

Fig. 1. Use of cryptography at IoT device level

Cryptography serves as a traditional means to safeguard data by utilizing encryption and decryption techniques. Encryption transforms the original data into ciphertext, an alternative form with a different meaning, shown in Figure 1. Even if an attacker obtains the ciphertext, they cannot access the original content. Decryption is used to change back the ciphertext to its original form for the intended recipient. Keys, or sometimes key pairs, are employed to unlock or decrypt the ciphertext. Authentication techniques are used to confirm the identity of entities seeking access. These cryptographic and authentication techniques are resource-intensive and may not be suitable for tiny IoT devices. Therefore, lightweight cryptographic techniques have been proposed as robust solutions for IoT-enabled devices [15].

Additionally, dedicated platforms are designed to provide data protection for both stored data and data in transit [16]. While primarily focused on security, these platforms also offer services such as data monitoring, management, and network administration. The security solutions offered by these platforms address aspects such as data integrity during transmission, device identification during connection requests, device identification during transit, and device/network/service authorization.

The utilization of AI and ML-based techniques presents another effective approach to mitigate emerging security threats and breaches in IoT devices and networks. ML algorithms can create models to identify data trends and make forecasts. Many ML algorithms operate at the gateway level to identify malware activities based on incoming traffic patterns [17]. Artificial Neural Networks (ANN), Support Vector Machines (SVM), and fuzzy logic are commonly employed under ML-based methods to protect data [18].

Although initially developed for financial transactions using cryptocurrencies, blockchain technology can be harnessed to enhance the security of IoT devices and networks due to its inherent security features. Blockchain offers decentralization, fixity, non-repudiation, clarity, and traceability. It strengthens IoT device security by digitally signing and encrypting stored and transmitted data using cryptographic keys. Additionally, blockchain utilizes smart contracts to address vulnerabilities in IoT devices or networks [19].

IV. CONCLUSION

IoT devices are susceptible to a range of security risks, including physical attacks, malware attacks, DDoS attacks, and data breaches. These dangers have the potential to seriously harm an organization's finances and image by jeopardizing its customers' security and privacy. Adopting a complete security approach that incorporates encryption, authentication, access control, and ongoing device monitoring of IoT devices is crucial to reducing security concerns on IoT. Every phase of the IoT device's life cycle, including design, manufacture, deployment, and decommissioning, must also include security measures. These dangers may also be reduced by informing end users of the value of IoT security and giving them the resources, they need to safeguard their devices. In conclusion, all parties involved in IoT must address the security concerns that are present. IoT security risks may be significantly decreased by taking a proactive strategy that includes deploying strong security measures, following best practices in IoT security, and training end users. Prioritizing IoT security is essential to ensuring that the potential security concerns do not outweigh the advantages of IoT.

V. ACKNOWLEDGMENT

The authors are thankful to Amity University Kolkata, India for the necessary support for this work.

VI. REFERENCES

[1] Al-Sarawi, S., Anbar, M., Abdullah, R., & Al Hawari, A. B. (2020, July). Internet of things market analysis forecasts, 2020–2030. In 2020 Fourth World Conference on smart trends in systems, security, and sustainability (WorldS4) (pp. 449-453). IEEE.

[2] Santamouris, M., &Vasilakopoulou, K. (2021). Present and future energy consumption of buildings: Challenges and opportunities towards decarbonisation. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 1, 100002.

[3] Murthy, K.S., Herur, P., Adithya, B., & Lokesh, H. (2018). IoT-Based Light Intensity Controller. 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), 455-460.

[4] Xie, C., Yu, B., Zeng, Z., Yang, Y., & Liu, Q. (2020). Multilayer internet-of-things middleware based on knowledge graph. IEEE Internet of Things Journal, 8(4), 2635-2648.

[5] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[6] Roy, S. (2017). Hardware Trojans–A Cause of Concern In Safety Critical Electronic Systems. Int. J. Modern Trend. Eng. Sci., 4(5), 110-119.

[7] Sidhu, S., Mohd, B. J., &Hayajneh, T. (2019). Hardware security in IoT devices with emphasis on hardware trojans. Journal of Sensor and Actuator Networks, 8(3), 42.

[8] Breier, J., & He, W. (2015, September). Multiple fault attack on present with a hardware trojan implementation in fpga. In 2015 international workshop on secure internet of things (SIoT) (pp. 58-64). IEEE.

[9] Das, D., Maity, S., Nasir, S. B., Ghosh, S., Raychowdhury, A., & Sen, S. (2017, May). High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 62-67). IEEE.

[10] Genkin, D., Shamir, A., &Tromer, E. (2017). Acoustic cryptanalysis. Journal of Cryptology, 30, 392-443.

[11] Ullah, I., Khan, N., &Aboalsamh, H. A. (2013, April). Survey on botnet: Its architecture, detection, prevention and mitigation. In 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC) (pp. 660-665). IEEE.

[12] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[13] Saad, R. M., Anbar, M., Manickam, S., & Alomari, E. (2016). An intelligent icmpv6 ddos flooding-attack detection framework (v6iids) using back-propagation neural network. IETE Technical Review, 33(3), 244-255.

[14] Retting, R. (2017). Pedestrian traffic fatalities by state. Governors Highway Safety Association: Washington, DC, USA.

[15] Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2016, January). Security analysis on consumer and industrial IoT devices. In 2016 21st Asia and South Pacific design automation conference (ASP-DAC) (pp. 519-524). IEEE.

[16] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[17] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., &Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

[18] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine, 35(5), 41-49.

[19] Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.

VII. BIOGRAPHIES

Aakash Acharjee (Male) was born in Kalyani, India. He did his master graduation from Amity University, Kolkata, India.

His special fields of interest included theory and application of Internet of Things, Sensor Networks, and Machine Learning. He has few good publications in the field of IoT applications. Also, he participated in many international conferences and presented papers on IoT applications.

Sabyasachi Mondal (Male) was born in Kolkata, India.

He is working as an Associate Professor in the Department of Mathematics, North-Eastern Hill University, Shillong, Meghalaya, India. Before joining here, he was a Postdoctoral Research Fellow in University of KwaZulu- Natal, South Africa. He completed his Ph.D. from Visva Bharati University, Santiketan, West Bengal, India. His research interests are on CFD, boundary value problems, nanofluid flows.

Rishabh Pipalwa (Male) was born in Howrah, India. He graduated from Amity University, Kolkata.

He was a student of integrated MCA from Amity University Kolkata. He has a keen interest in research areas. His research area is Sensor network, Internet of things, Machine Learning in the field of Health Informatics. He has publications in many Journals and Conference proceedings. He is working on many research areas with various professors at Amity University Kolkata and IIT Kharagpur on various topics.

Arjun Mitra (Male) was born in Suri, India.

He is a student of BCA from Amity University Kolkata. He has a keen interest in many research areas like Sensor network, Internet of things, Machine Learning etc. His publications are mainly in the field of sensor networks.

Abhijit Paul (Male) was born in Kumarghat,Tripura, on December24, 1984. He is graduated from the Gurucharan College, Silchar, Assam, India.

His employment experience included the Assam Downtown University, Guwahati, India and Amity University, Kolkata, India. His special fields of interest included sensor network, Internet of Things and Ad hoc network.

Dr. Paul received Ph.D. degrees from Assam University, Silchar, India. He has published many research articles in reputed journals and conferences. Also, he is a reviewer of many reputed journals.