A CRITICAL ANALYSIS OF SECURITY REQUIREMENTS OF IOT

Vinit Kumar[1], Mr. Gaurav Kumar Saxena[2]
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer Science & Engineering School of Engineering, Sri Satya Sai University Of Technology & Medical Sciences, Sehore (M. P.)
[2]Department of Computer Science & Engineering School of Engineering, Sri Satya Sai University Of Technology & Medical Sciences, Sehore (M. P.)
way2vinit@gmail.com[1] gaurav.saxena18@gmail.com[2]

* Corresponding Author: Vinit Kumar

Abstract: *This study conducts a thorough examination of the security requirements intrinsic to the Internet of Things (IoT) landscape. In an era of interconnected devices, the necessity for robust security protocols is paramount. The research scrutinizes various facets, including data integrity, confidentiality, and availability, to identify vulnerabilities and potential threats within IoT systems. Employing a critical lens, the study delves into existing security frameworks and assesses their efficacy in mitigating evolving risks. Furthermore, it explores emerging technologies and novel methodologies, offering insights into adaptive security measures. By critically analyzing the security requirements of IoT, this research contributes to the ongoing discourse on safeguarding digital ecosystems, providing a foundation for future advancements in securing the IoT landscape.*

Keywords: *Internet of Things (IoT), Security Requirements, Critical Analysis, Security Frameworks.*

1. INTRODUCTION

Although there was an inconsistency in the definition of the Internet of things, technology is a technology that combines daily things connected to sensors in heterogeneous networks. According to [1] IoT has limited human intervention. Technology for shining the technology and cyberspace environment. Physically, the data was exchanged when collecting, generating or processing important data for its cyberspace function. The sensors collected consumer safety or privacy-sensitive data. This can affect legal concern [1] In addition, the authors affirmed that the development of software or the configuration control in the IOT sensors could affect the concerns of cybersecurity in that host network.

The manufacturers were delayed by the safety regulations and recently had government interventions only if they are associated with the cybernetic security of IOT [2]. Government agencies have feared the severe industry in the industry by carrying out regulations, and the Government of the United States promoted a safe development adopted by a supplier adopted for future work [2].

The Bluetooth wireless communication industry has grown to a place where technology incorporates the sensor to many devices, including mobile devices, wearables and vehicles. There were many integrations of technology and security updates, including version 4.2 of Bluetooth Low Energy (BLE), including version 4.2 of Bluetooth Low Energy (BLE). BLE focused on increasing security posture for low power requirements of the channel jump and previous versions, and was a communication protocol for the IoT Communication Protocol [3]. The manufacturer of the IOT device contains BLL using BLE technology and IOT sensors embedded. For paper experiments, the BLE protocol used version 4.2.The proliferation of interconnected devices in the modern era has ushered in a new age of technological convenience and efficiency, encapsulated by the Internet of Things (IoT). As our reliance on IoT ecosystems grows, so does the imperative to fortify these networks against evolving cyber threats. This study embarks on a critical analysis of the security requirements intrinsic to IoT, recognizing the vital need for robust safeguards in the face of escalating risks.

The introduction outlines the transformative impact of IoT on various industries and daily life, emphasizing the unparalleled connectivity it facilitates. With this heightened connectivity, however, comes an increased susceptibility to cyber threats, ranging from data breaches to unauthorized access. The critical analysis aims to dissect the multifaceted security demands of IoT, considering the triad of data integrity, confidentiality, and availability.

As the research unfolds, it navigates through existing security frameworks, scrutinizing their effectiveness and identifying potential gaps. This critical exploration is not merely retrospective; it extends to the forefront of emerging technologies and innovative methodologies, aiming to discern adaptive measures capable of addressing the dynamic landscape of IoT security.By delving into the intricacies of security requirements in the realm of IoT, this critical analysis seeks to provide a foundation for understanding the challenges and opportunities inherent in securing these interconnected systems. The insights gleaned from this study are poised to contribute significantly to the ongoing discourse on fortifying the digital infrastructure that underpins our interconnected world. The source used by the IOT sensors started with a device-level attack and the attacker abused usability in the code and firmware bugs [4]. The attacks used the IoT sensor through a serious Bluetooth attack. The strategy requires user intervention to disable Bluetooth when not in use. According to [5],IoT middleware sensors act as a bridge between physical and virtual resources that do not have the same control over security. due to low consumption and lack of code [5] Exploitation is due to poor deployment criteria or lack of tight configuration control [5]. Attackers deployed a wide range of issues using a large number of vulnerable sensors [5]. a bridge between middleware and memory-related vulnerabilities, triggered a buffer overflow attack against a specific sensor. By exploiting memory, an attacker allows a memory executable to deliver malicious content, wrapper code, or vulnerable sensors.The execution of malicious code allows an attacker to monitor or deploy software on a target IoT sensor [3]. According to [6], Commands and Controls (C2) by which sensor nodes create complex networks through agent-based self-organization models by implementing predefined rules, the result is an agent-based model that integrates expected behavior and uncovers opportunity. to deploy penetration testing tools [6]. Self-organization, not controlled by external sources, is formed by setting up complex sensor networks [6]. If a sensor change occurs, it adapts to the newly defined rules. The attacker has a set of malicious rules that override predefined steps to force spoofing to create a sensor. Fake IoT variables [6], .Problem Statement for BLE IoT Sensors A common problem is that IoT sensors are vulnerable to cyberattacks [3]. The specific issue is that IoT sensors have many security concerns due to BLE encryption vulnerability, leading to cybersecurity attacks [3] UKMinistry of Digital Culture, Media and Sports, 2018) The combination of known Bluetooth vulnerabilities and limited security guidance has proven to be an issue as these vulnerabilities expose IoT sensors to attacks. The network is publicly available. (2018) presented 20 known attack vectors using IoT sensors with BLE communication protocol to exploit vulnerabilities in their implementation. IoT devices are delayed with security controls and lack standard security monitoring (UK.Department of Culture, Media and Digital Sports, 2018).

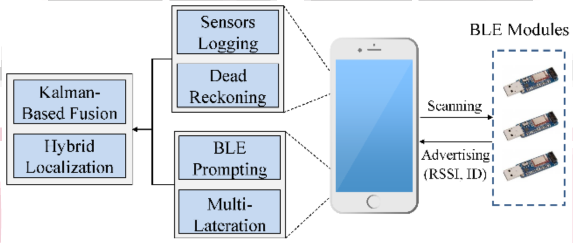

Figure:1 Improved BLE Indoor Localization

2. LITERATURE REVIEW

The first titles searched included “Securing the IoT Bluetooth Low Energy,” “Defensive Strategies for the IoT Bluetooth Low Energy,” and “Self-organized IoT devices to defend against cyber threats.” Keyword searches completed the literature review documented in Appendix A and Table 3. The following hypothesis and research question guided the literature review. The application of NIST security controls and best practices for the IoT sensors using BLE would not adequately protect the devices from exploitation, leveraging well-known Bluetooth attacks.

Additionally, the null hypothesis was applying NIST security controls, and best practices for securing IoT sensors using the BLE device would mitigate well-known Bluetooth attacks. The historical documentation, research articles, journals, and publications suggested there are significant problems within the IoT and lead the researcher to answer “Will the application of NIST recommended security controls and best practices mitigate the success of well-known attack vectors on IoT sensors using BLE?” According to the Internet of Things: Privacy & Security in a Connected World (Federal Trade Commission, 2015), security risks included disclosure of Personally Identifiable Information (PII), attacks critical infrastructure, and risks to personal security were concerns in emerging IoT technology. Storing account and financial information on Smart TVs during internet browsing could expose users to information disclosure (Federal Trade Commission, 2015). According to the Federal Trade Commission (2015),trust relationships and interconnection of the IoT sensors were a concern because vulnerable sensors create vulnerabilities for protected IoT nodes.

The “Internet of Things: a security point of view” . conducted an extensive qualitative study on the software vulnerabilities in IoT and concluded there would need to be a future study on defensive strategies to build a framework. The study established a framework modeling four-layers focusing on sensors, communication, network, and software security .. The researchers stated within an enterprise where IoT sensors exist, and it may be vulnerable to data breaches. Li concluded the review by generalizing the need for defensive framework experimentation in IoT [10]. Within the evaluation, communication occurred through HTTP or an unencrypted link susceptible to information disclosure [10].

“A Guide to Bluetooth Security” [8]provided information on security capabilities and provided security recommendations for Bluetooth communications. Bluetooth beacons designed to run on battery power and deployed for use during an extended period [8] . Beacons maintained up to a 30- meter (100 foot) range to establish a connection [8] .BLE operated on 40 channels and used AES-CCM for authentication and encryption [8] .In BLE, a Piconet was set up for the local Wireless Personal Area Network (WPAN) [8] . Piconets have the highest device limit of 7 active sensors;

however, they can have 255 stored sensors [8] . Slave sensors of one Piconet can be the master of another, creating a network chain [8] . BLE sensors can send connectionless broadcast data to all nodes within the Piconet [8] .
While there were many different types of attacks for Bluetooth, an important note to take is the version of the sensor [3]. An outdated Bluetooth sensor places the entire Piconet at risk for exploitation [3] Secure BLE sensors communicating with weak sensors would not protect the connection and is as strong as the weakest device [4] documented well known Bluetooth attacks from a holistic view from early Bluetooth implementation to the present-day risks represented spoofing, pin cracking, eavesdropping, unauthorized disclosure of data, configuration software management and physical security. NIST security guidance and control documented countermeasures of some attacks through the Mobile Threat Catalogue.
In “Securing the Internet of Things: Challenges, Threats and Solutions” [11] defended the software-defined network for an IoT network had limitations when deploying Security Information and Event Management (SIEM) technologies; due to the amount of data processing it did, effective monitoring and alerts on malicious traffic produced a large number of alerts [11]. In “Shielding IoT against cyber-attacks: An event-based approach using SIEM”[12]stated Intrusion Detection System (IDS) solutions which reported security incidents to a SIEM had issues with limited hardware resources on IoT sensors, their protocol stack, and generating massive amounts of data. Accurate reporting of security incidents with an IDS did not use Bayesian inference to filter data for processing [12]. Therefore, the researchers evaluated multiple open-source IDS products to perform Incident Response, including Suricata, OpenVAS, and Kismet IDS, sending IoT alerts to OSSIM [12]. contributed static correlational rules for IoT security architecture used with Incident Response. The rules addressed the mapping of software vulnerabilities, security events, and attack surfaces to specific IoT devices and sensors [12].

3. COMPARATIVE ANALYSIS

Security Frameworks:
Evaluate widely adopted security frameworks such as ISO/IEC 27001 and NIST Cybersecurity Framework in the context of IoT.Compare their applicability to the unique challenges posed by IoT, considering factors like scalability, adaptability, and integration capabilities.

Authentication and Authorization Mechanisms:
Examine different authentication and authorization protocols employed in IoT security, such as OAuth, JWT, and X.509 certificates.Compare their effectiveness in ensuring secure access and data protection within the diverse and dynamic IoT environment.

Encryption Techniques:
Analyze encryption algorithms commonly used in IoT, such as AES and ECC. Compare their efficiency in safeguarding data transmitted between IoT devices, considering factors like computational overhead and energy consumption.

Device Management and Lifecycle Security:
Evaluate approaches to device onboarding, provisioning, and decommissioning. Compare methods for ensuring the security of IoT devices throughout their lifecycle, addressing issues like firmware updates, patch management, and secure disposal.

Data Integrity and Privacy:
Assess mechanisms for ensuring the integrity of data transmitted and stored by IoT devices. Compare privacy-preserving techniques, including anonymization and differential privacy, to safeguard sensitive information

Resilience Against Cyber Attacks:
Explore the resilience of IoT systems against common cyber threats like DDoS attacks and malware.
Compare strategies for anomaly detection, intrusion prevention, and incident response in different IoT security paradigms.

Regulatory Compliance:
Consider compliance requirements imposed by regulations like GDPR and HIPAA in the context of IoT.
Compare how various security approaches align with and support compliance with these regulations.
User Education and Awareness:

Analyze the role of user education and awareness in IoT security.
Compare the effectiveness of different strategies in ensuring that end-users and stakeholders understand and adhere to security best practices. By conducting a comprehensive comparative analysis across these dimensions, one can gain a nuanced understanding of the strengths and limitations of existing security approaches in meeting the unique challenges posed by the Internet of Things. This insight is crucial for shaping future security strategies and ensuring the continued integrity and resilience of IoT ecosystems.

4. DISCUSSION AND FINDINGS

Vulnerability Assessment:
The study undertook a comprehensive vulnerability assessment of IoT ecosystems, identifying potential weak points in data transmission, storage, and device communication. This analysis involved an examination of both known vulnerabilities and potential emerging threats.

2. Existing Security Frameworks:
The findings reveal a diverse landscape of existing security frameworks in use for IoT. These frameworks were critically evaluated in terms of their adaptability, scalability, and effectiveness in safeguarding against current and anticipated threats. Notable frameworks such as IoT Security Foundation, OWASP IoT Top 10, and others were scrutinized for their strengths and weaknesses.

3. Data Integrity Challenges:
The discussion highlights challenges related to ensuring data integrity within IoT systems. Factors such as data tampering, unauthorized access, and data corruption were explored. The findings suggest that maintaining the integrity of data in transit and at rest remains a critical concern that necessitates innovative solutions.

4. Confidentiality Measures:
The study delves into the measures employed to uphold data confidentiality in IoT environments. Encryption protocols, access controls, and secure communication channels were examined. The discussion addresses the effectiveness of these measures and potential improvements to bolster confidentiality in the face of evolving cyber threats.

5. Availability Considerations:
Ensuring the availability of services and data in IoT ecosystems emerged as a pivotal aspect of the analysis. The study scrutinized potential disruptions, including denial-of-service attacks and network outages, and proposed strategies for enhancing the availability of critical IoT functions.

6. Emerging Technologies and Adaptive Solutions:
The discussion explores emerging technologies, such as blockchain, artificial intelligence, and machine learning, as potential game-changers in IoT security. The findings emphasize the need for adaptive security solutions that evolve alongside emerging threats, and the study provides insights into how these technologies can be harnessed for improved security.

7. Regulatory and Compliance Landscape:
The study also investigates the regulatory and compliance landscape surrounding IoT security. Findings highlight the importance of aligning security measures with industry standards and legal frameworks. The discussion emphasizes the role of regulatory compliance in promoting a baseline of security across diverse IoT deployments.

5. **CONCLUSION**

In essence, this critical analysis provides a roadmap for fortifying the security of IoT ecosystems. By understanding the nuanced challenges and opportunities inherent in IoT security requirements, stakeholders are better equipped to implement measures that not only address current vulnerabilities but also anticipate and adapt to the ever-changing threat landscape. As the IoT continues to shape our interconnected world, the findings of this study contribute to the ongoing dialogue on ensuring the integrity, confidentiality, and availability of data within these dynamic and vital systems.

References

[1] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC). Retrieved from https://www.internetsociety.org/wp- content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdfAlgorithm_Based_on_Aes_RSA_and_Twofish_for_Bluetooth_Encryption

[2] Hogan, M., & Piccarreta, B. (2018). Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT) (No. NIST Internal or Interagency Report (NISTIR) 8200 (Draft)). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

[3] Lonzetta, A., Cope, P., Campbell, J., Mohd, B., & Hayajneh, T. (2018). Security vulnerabilities in bluetooth technology as used in iot. Journal of Sensor and Actuator Networks, 7(3), 28. doi:10.3390/jsan7030028

[4] Fernandes, E. (2017). Securing Personal IoT Platforms through Systematic Analysis and Design. (Doctoral Thesis). Retrieved from ProQuest Database. (Accession No.10612074) Retrieved from https://deepblue.lib.umich.edu/handle/2027.42/137083

[5] Freemantle, P., & Scott, P. (2017). A survey of secure middleware for the Internet of Things. PeerJ Computer Science, 3, e114. doi:10.7717/peerj-cs.114

[6] Batool, K., & Niazi, M. A. (2017). Modeling the internet of things: A hybrid modeling approach using complex networks and agent-based models. Complex Adaptive Systems Modeling, 5(1), 4. doi:10.1186/s40294-017-0043-1

[7] Creswell, J. W. (2002). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Prentice-Hall.

[8] Padgette, J., Scarfone, K., & Chen, L. (2017). NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security. doi:10.6028/nist.sp.800-121r2

[9] Franklin, J. M., Howell, G., Boeckl, K., Lefkovitz, N., Nadeau, E., Shariati, D., ... & Peck, M. (2019). Mobile device security corporate-owned personally-enabled (COPE).

[10] Tzezana, R. (2017). High-probabi.(Barcena & Wueest, 2015). ty and wild-card scenarios for future crimes and terror attacks using the Internet of Things. foresight, 19(1), 1-14. doi:10.1108/FS-11- 2016-0056

[11] Grammatikis U.K. Department for Digital Culture, Media & Sport. (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

[12] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., … Gómez Mármol, F. (2018). Shielding iot against cyber-attacks: An event-based approach using siem. Wireless Communications and Mobile Computing, 2018, 1-18. doi:10.1155/2018/3029638

[13] Stanislav, M., & Beardsley, T. (2015). Hacking iot: A case study on baby monitor exposures and vulnerabilities. Retrieved from Rapid7 website https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-ulnerabilities.pdf

[14] Ometov, A., Solomitckii, D., Olsson, T., Bezzateev, S., Shchesniak, A., Andreev, S., & Koucheryavy, Y. (2017). Secure and connected wearable intelligence for content delivery at a mass event: a case study. Journal of Sensor and Actuator Networks, 6(2), 5. doi:10.3390/jsan6020005

[15] Askov, E. N. (1985). Single-subject, multiple-baseline designs in evaluating adult literacy programs (ED264441). ERIC. https://eric.ed.gov/?id=ED264441

[16] Mwathi, D. G., Okelo-Odongo, W., & Opiyo, E. (2017). Vulnerability analysis of 802.11 authentications and encryption protocols: cvss based approach. International Research Journal of Computer Science, IV(VI),

[17] Elia, I. A., Antunes, N., Laranjeiro, N., & Vieira, M. (2017, September). An analysis of openstack vulnerabilities. In 2017 13th European Dependable Computing Conference (EDCC) (pp. 129-134). doi:10.1109/EDCC.2017.29