Study of IoT Layers Vulnerabilities and Attack Surfaces

Mr. Karan Tamboli[a], Dr. Vanita Mane[b], Mrs. Namita Pulgam[c] and Dr. Tabassum A. Maktum[d]

Department of Computer Engineering, Ramrao Adik Institute of Technology,
Dr. D. Y. Patil Deemed to be University, Nerul, Navi Mumbai, India

Abstract: The rapid surge in the adoption of Internet of Things (IoT) devices and their use in many areas has revolutionized the way humans interact with technology such as embedding connected devices into the diverse aspects of our lives. However, this adoption has also opened up a portal for cyber security threats as IoT security vulnerabilities and attack surfaces have become a critical concern. This study is towards the view of landscape of IoT security, exploring the various vulnerabilities present in the IoT devices, networks and overall ecosystems, examines the overall view of most pre-known vulnerabilities, such as weak authentications, encryption, protocols and attacks con-ducted over IoT infrastructure such as Botnet, Man in the Middle (MIM) and many more. The analysis of Layers and Protocols used in IoT and it's summarizing aims towards research, raise awareness and to promote the development of adequate security measures to prevent the rapidly evolving IoT.

1 INTRODUCTION

The Internet of Things (IoT) which has seen massive developments in past years is revolutionizing the way we interact with the devices and the surrounding environment. a network of physical components, systems and the devices that are connected with each other can communicate and share or exchange data over the Internet is known as the Internet of Things (IoT). The Automation and convenience could be increased by IoT technology in many different industries, including smart cities, transportation, healthcare, and agriculture but despite the potential for revolutionary advancements in technology, IoT poses security risks and attack surfaces that compromise the confidentiality, availability, and integrity of data and services. This study aims to explore the architecture of IoT systems, towards into their various layers of an IoT and comprehensively examines the vulnerabilities within these layers and the protocols [1] that can potentially lead to attacks and also user privacy threats [2] in evolving nature. While studying the vulnerabilities with possible

attacks and the causes referenced to each of significant layers of IoT and protocols [26] used and conclusively propose the possible mitigation measures to prevent and secure the IoT environment. This comprehensive study is towards the expansive landscape of IoT security, aiming to the multifaceted vulnerabilities of IoT devices, networks and the ecosystems they create. Goal of this exploration is to highlight awareness and action. By deeper under-standing of these rapidly evolving IoT landscape vulnerabilities, this research aims to prompt the development of robust, adaptive security measures. The Wider layers of IoT has been explained differently from basic Layered of IoT and the Protocols[3] used to make this IoT system work and their potential demerits or concern factors which invokes a summarized form of input to deal with and possible mitigation has been discussed in classified form. The aim of study is to enhance awareness and understanding of the security challenges in IoT architecture among stakeholders, including developers, policymakers and end-users. To identify and categorize the various security vulnerabilities present in IoT systems and assess their potential risks.

[a] https://orcid.org/0009-0008-7646-0448
[b] https://orcid.org/0000-0002-4303-4089
[c] https://orcid.org/0000-0001-7725-0997
[d] https://orcid.org/0000-0002-8797-2894

By Examining the attack surfaces [18] related to these vulnerabilities and the potential attack ways and malicious methods and to improve the overall security of IoT ecosystems and possibly to propose the mitigation methods to IoT security vulnerabilities, best practices and study possible strategies are being mentioned.

The objective of this study is to review various studies conducted before in IoT architecture layers and security and form a detailed layered structure from it and envelope an table with layers and their protocols as well as Vulnerabilities in it, and suggest possible mitigation Strategies in one shell from those.

2 LITERATURE SURVEY

In an examination while study of IoT Security an author Abid [1] provide a comprehensive analysis of the challenges linked with the IoT security including the device and their constraints and also the absence of standardized protocols in the vast landscape of Security. While The Muhammad Guezzaz [2] underscores the role of robust authentication mechanisms and encryption techniques for miti-gating of vulnerabilities within IoT ecosystems while also discussing potential drawbacks such as resource overheads etc. Author H.J Felcia [3] discusses about traditional internet of things infrastructure and proposing for the integration of innovative countermeasures and mentioned both the merits and limitations of existing solutions while the Selvakumar Manickam [4] directs an attention to the security of the MQTT protocol and highlighting resource constraints as a barrier to its widespread adoption and discussing potential trade-offs in security measures. P. Goyal [5] discuss the scope by addressing security threats across various layers of the IoT architecture, discusses for the implementation of security solutions like blockchain and machine learning and acknowledging the complexity and potential integration and challenges. Author Forhad et al. [6] studies the security needs of IoT devices and about the importance of approach to ad-dressing vulnerabilities across various OSI layers along with the challenges in the implementing those measures effectively. T. Lestable [7] focuses on safeguarding privacy within smart homes and the concerns over manufacturers to prioritizing market share over security measures but talks about necessitating the development of robust security frameworks to protect the user data and discussing potential trade-offs in usability of IoT systems. A. Murali Rao [8] provides

the perspective on IoT's interconnected systems underscoring the role of ongoing re-search efforts in IoT systems against emerging threats and vulnerabilities and also discussing the challenges in rapid technological advancements. The authors [9] reviews IoT security patterns and architectures, identifying areas for improvement and inputs for enhanced collaboration between academics and industry stakeholders to secure the IoT security. Authors O. Toutsop, S. Das and K. Kornegay [10] studies into the threat modelling methodologies and on potential security pitfalls within home-based IoT devices and proposing strategies to enhance system resilience and integrity, while also discussing potential challenges in implementing and maintaining such methodologies effectively. A. Majid [12] discusses security prerequisites which are critical for safeguarding Smart City IoT systems while utilizing the STRIDE framework to identify and address potential security vulnerabilities across the IoT deployments and also discusses potential challenges in implementing and maintaining such type of measures effectively in IoT.

3 BACKGROUND

IoT (Internet of Things) architecture is a framework that defines the structure and components of a system designed to connect and manage a multiple node objects and devices through the Internet. It contains the hardware, software and communication protocols necessary for data exchange and to control over the internet-connected devices[5]. The Figure 1 Shows Basic Architecture of IoT Ecosystem widely discussed in section 3.1
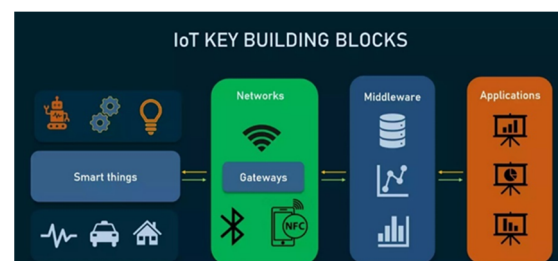

Figure 1: IoT Architecture[15].

3.1 Basic Layers of IoT Architecture

Perception Layer is the lowest layer in the IoT architecture and involves the physical 'things" or devices that collect data from the real world these

devices can include sensors, actuators, cameras, RFID tags and many more devices the sensors gather data from the environment such as temperature, humidity, light, motion etc and actuators are takes the actions based on the data received, such as turning on/off a light etc[9].

Network Layer is used for transmitting data from the perception layer to higher layers of the IoT system. It involves various communication protocols and technologies[21][26] including wired (e.g., Ethernet) and wireless (e.g., Wi-Fi, Blue-tooth, Zigbee, cellular) connectivity options an Gateways be used for communication between different types of devices and protocols[21].

Middleware Layer acts as an intermediary between the network layer and the application layer handles the tasks such as data processing, data transformation, and the protocol translation the Middleware include computing for real-time data analysis and decision-making at the device level itself.

Application Layer is the topmost layer where IoT applications and services are developed and deployed. The IoT applications can be from simple data monitor-ing and reporting to analytics of automation and control systems. An data from sensors and devices are processed, analysis and used to do actions or generate insights.

3.2 Wider Layers of IoT Architecture

Sensors and Devices Layer: Foundation of IoT interfaces directly with the physical environment to collect data from diverse sensors and devices. Security vulnerabilities include weak authentication, sensor spoofing and physical tampering, which compromise data integrity and system functionality, in recent due to weak authentication the Numerous incidents in 2020 showed that Ring door-bells[30] were hacked due to many users did not change the default passwords which allows unauthorized access to video feeds in another sensor spoofing in 2021 research demonstrated how Autopilot system[31] could be tricked by spoofing sensor data while the key protocols used such as MQTT [16][29] and CoAP.

Connectivity Layer: This layer used for communication, channelling in be-tween IoT devices and the network and has options like Wi-Fi, cellular and other connectivity solutions while the Security

vulnerabilities in this layer are insecure network protocols, device spoofing and eavesdropping which poses risks to data confidentiality and system security, examples in recent like Insecure Network Protocol in 2020 vulnerabilities in the Z-Wave protocol which is widely used by smart home devices were exposed which allows attackers to intercept and alter device communications in CVE-2019-9494 and Device Spoofing vulnerability in Apple's Air-Drop to devices and access person-al information reported in CVE-2019-8615, the protocols like HTTP/HTTPS[16] and DTLS for communication [24] used.

Middleware Layer: Acts as an intermediary manages data processing, protocol translation and seamless communication between IoT devices and applications. Vulnerabilities include insecure data handling, message spoofing and unauthenticated access, which compromise system integrity and expose sensitive information in recent times the Insecure Data Handling at 2021 a vulnerability was identified in the implementation of the MQTT protocol across several IoT plat-forms making it possible to intercept and manipulate messages reported in CVE-2019-11779 while the Message Spoofing in 2020 the Philips Hue smart lights were found to be susceptible to Zigbee protocol exploits to allowing attackers to spoof messages and control the lights in reported CVE-2020-6007 as the Key protocols such as MQTT and AMQP used within the middleware [19].

Application Layer: It is central to IoT which processes and analyses data for insights. Security vulnerabilities includes in this layer is data breaches, vulnerabilities in machine learning algorithms and inadequate access controls poses the risks to data confidentiality and system reliability context to a significant breach in 2021 involved Verkada security cameras[32] which exposes live feeds from thousands of cameras in various sensitive locations due to poor application security and Vulnerabilities in Machine Learning Algorithms[33] attacks on facial recognition systems used by smart security cameras were causing them to misidentify individuals the Protocols like RESTful APIs and gRPC which facilitate data exchange are used [26] [21].

Integration Layer: Used for seamless integration of IoT data into existing IT systems and external services across diverse platforms. The Vulnerabilities include insecure APIs, data leaks and inadequate data mapping, leading to data

inconsistencies and breaches during integration in recent times examples Inse-cure APIs was found that Peloton's API[34] which exposed private user information such as age, gender and location due to inadequate authentication while the Data Leaks in smart meter integrations with utility systems in the UK led to the exposure of personal user data, the Protocols like HTTP/HTTPS and Web-Socket [23][28] which used.

Business Layer: It shows the IoT's impact on operational efficiency, revenue generation and innovation in business models Security, the vulnerabilities include data monetization risks, financial data security concerns and subscription fraud which poses threats to revenue streams and customer trust such as Financial Data Security In 2019, smart payment systems used in vending machines were found to have vulnerabilities that allowed unauthorized transactions and Subscription Fraud in 2021 a vulnerability in the subscription models of certain IoT services allowed attackers to bypass payments and access premium features without authorization while the protocols HTTP/HTTPS and MQTT [5] [19] are used.

Security Layer: It is a foundational for IoT security which implements measures like authentication, authorization and data encryption to protect system integrity and confidentiality. The Vulnerabilities include weak authentication, lack of data encryption and inadequate access controls, exposing systems to un-authorized access and data breaches Weak Authentication In 2020 leads to vulnerabilities in authentication mechanisms of several smart home hubs were al-lowing unauthorized access and control over devices reported in CVE-2020-16136 while due to the Lack of Data Encryption In 2021, some IoT medical de-vices were found to be transmitting patient data without encryption exposes sensitive information, the protocols used such as TLS/SSL and OAuth[17].

Management and Monitoring Layer: Used as device monitoring, maintenance and firmware updates to ensure the health and security of IoT devices and systems. An Vulnerabilities include insecure device management, unsecured firm-ware updates and unauthorized access to IoT platforms, compromising system security and functionality such as Insecure Device Management attracts vulnerabilities in the management platforms of various smart camera systems allowed unauthorized access and control and incident in Unsecured

Firmware Updates In 2021 a flaw in the firmware update process of some IoT routers was discovered which enabling attackers to install malicious firmware. CVE-2020-28592 while protocols like HTTP/HTTPS and MQTT [12] used.

User Interface Layer: This used as interfaces for users to interact with IoT data, enhancing user experience and decision-making the Security vulnerabilities include insecure user authentication, data exposure and cross-site scripting, posing risks to user privacy and system integrity into the protocols like HTTP/HTTPS and WebSockets enable secure communication and real-time data exchange in user interfaces [25].

Regulatory and Compliance Layer: This layer addresses legal and aspects of IoT operations ensuring compliance with data privacy regulations and industry-specific standards while Vulnerabilities include data privacy violations, non-compliance with regulations and ethical concerns regarding data collection and usage, examples such as Data Privacy Violations In 2021 data privacy violation was discovered when a smart toy company was found to be collecting and storing children's data without parental consent and violating COPPA regulations and Non-Compliance with Regulations in 2020, several smart medical devices were found to be non-compliant with HIPAA, risking patient data exposure while the most used protocols like HTTP/HTTPS[12] and TLS/SSL [18].

4 KEY FINDINGS AND ANALYSIS

4.1 Concerns and Findings in Layers and Protocols

In the IoT architecture, different layers utilize specific protocols to enable communication, each facing distinct privacy and security challenges. For instance, at the a Sensors and Devices Layer MQTT and CoAP are used where the main concern is unauthorized access to sensitive sensor data as seen in example of them, In the Connectivity Layer the HTTP/HTTPS and DTLS protocols used for data data transmission but concerns are eavesdropping and privacy breaches. The Middleware Layer MQTT and AMQP have risks like data tampering and unauthorized access which can potentially compromising data integrity. Likewise the Application Layer where RESTful APIs and gRPC

are used the vulnerabilities like SQL injection poses a threats to stored user data security. The Integration Layer utilizes protocols like HTTP/HTTPS and WebSocket has risks such as data leak-age through APIs or intercepted communication. In the Business Layer where the HTTP/HTTPS and MQTT protocols are used there are unauthorized access potentially leads to the data theft and compromising sensitive business information. while, the Security Layer uses TLS/SSL and OAuth protocols face issues such as weak authentication and unauthorized access so safeguarding user data from breaches is important. In the Management and Monitoring Layer where the HTTP/HTTPS and MQTT protocols are used has concerns about unauthorized access to device management systems is important to use secure device management practices, In the User Interface Layer protocols are HTTP/HTTPS and Web-Sockets which face the risks like unauthorized access and data leakage which needs security measures to implanted properly. In the end layer Regulatory and Compliance Layer which uses HTTP/HTTPS and TLS/SSL protocols needs compliance with data privacy regulations to avoid legal consequences and protect user data and the privacy.

The Table 1 outlines various attack surfaces and types of attacks within the context of IoT (Internet of Things) environments. This table consists of view of the threat landscape, including the potential impacts on both end users and the IoT ecosystem, The study is being conducted from the various segregated previous research and maps in overall context to different layers we have discussed in wider study of IoT layers.

In Table 1 we referenced vulnerabilities with respect to specific protocols and layers of the IoT architecture, security threats within this rapidly evolving domain. The Attack Types gives view of various types of attacks performed over the various layers of IoT and their possible impact on end users and on IoT environment and also the protocol which is used in that specific layer or has vulnerability which is used to perform such attack is referred with specific protocol is discussed widely.

Table 1. Attack Types and Impact Table.

SR	Attack Type	Impact on End User and IoT Environment	Protocols and Layers (References)
1	Data Tampering	**End User:** Data integrity compromised. **IoT:** Misleading data.	MQTT (Sensors and Devices Layer) [3][4]
2	Man-in-the-Middle (MitM)	**End User:** Confidential data exposure. **IoT:** Data compromise.	MQTT (Sensors and Devices Layer), WebSocket (Integration Layer)[3][5]
3	Unauthorized Access	**End User:** Privacy invasion. **IoT:** Unauthorized control.	CoAP (Sensors and Devices Layer), HTTP (Connectivity Layer)[5][9]
4	SQL Injection	**End User:** Data leaks. **IoT:** Database corruption.	RESTful APIs (Application Layer)[5][6]
5	Data Leakage	**End User:** Privacy breach. **IoT:** Sensitive data exposure.	HTTP (Integration Layer),(User Interface Layer)[3][4]
6	Subscription Fraud	**End User:** Financial losses. **IoT:** Revenue loss.	MQTT (Business Layer)[3]
7	Firmware Tampering	**End User:** Device malfunctions. **IoT:** Security compromise.	MQTT (Management and Monitoring Layer)[5]
8	XSS Attacks	**End User:** Browser-based attacks. **IoT:** Web interface compromise.	WebSockets (User Interface Layer)[5][6]
9	Regulatory Non-compliance	**End User:** Privacy violations. **IoT:**Legal repercussions.	TLS/SSL (Regulatory Compliance Layer)[4][6]
10	Ethical Violations	**End User:** Ethical concerns. **IoT:** Reputation damage.	TLS/SSL (Regulatory Compliance Layer) [3][4]
11	Denial of Service (DoS)	**End User:** Service unavailability. **IoT:** Network congestion.	MQTT (Middleware Layer)[3][4]
12	Device Spoofing	**End User:** Unauthorized access. **IoT:** Security breach.	CoAP (Sensors and Devices Layer), DTLS (Connectivity Layer)

4.2 Importance and Need of Implications of Data and Privacy in the IoT

Compliance with the data privacy regulations boards such as GDPR, CCPA and HIPAA is important, as failure to comply with these regulations can result in legal issues[17] and can leads to the fines and legal actions against the organizations or development companies, to build and maintain an user trust is important and should be main objective for businesses and institutions. The Instances such as the data breaches can break the trust of user which leads to non recover damage to organization's reputation and credibility also the financial implications of data breaches are significantly large which consist of expenses like legal fees, compensations to affected individuals and costs relating to recover the breach, these kind of breaches can cause in large financial losses for an organization.

The IoT often involves the collection of sensitive data like personal and financial information and health related data, Safeguarding this data isn't just a legal problem but also a moral and ethical issues with it. while ensuring safe operation with it is crucial as security breaches can disturb regular operations which are leads to downtime of system that can impact on overall productivity and services which affects an organization's efficiency also the Unauthorized access of user data can be results in identity theft, which has the severe consequences for individuals, so protecting user data is critical to prevent such instances.

Fail to comply with data privacy regulations not just pose legal risks but it can also lead to regulatory penalties and imposing financial issues on organizations and potentially affecting their sustainability in market, so to collaborate with the above concerns, vulnerabilities and causes it needs to look into a generalized solution to protect the attacks caused in various layers of IoT, The Possible Mitigation section gives a generalized view of suggested measures for attack vector type and layers and their protocols.

4.3 Protective Measures

Safeguarding the integrity of IoT landscapes needs a multi-faced approach which incorporating in various pre-known protective strategies. The below mentioned measures consist generalized authentication methods, data encryption practices and access controls which aimed at pre-defences against unauthorized access and potential data breaches. Integrating these protective strategies throughout the lifecycle of IoT projects establishes a sturdy security foundation, mitigating vulnerabilities and enhancing overall security standards across the IoT.

The Measures such as Implementing Strong Authentication, Encrypting Data in Transit and at Rest, Applying Access Controls and Role Based Permissions, Regular Firmware and Software Updates, Ensuring Network Security[22] with Firewalls and Regular Assessments, Prioritizing Privacy[26] Considerations from Design Stage, Educating Users and Employees on Security Best Practices, Utilizing Established IoT Security Frameworks and Guidelines, Securing Device Lifecycle from Manufacturing to Disposal, Promoting Ethical Data Collection and Usage, Deploying Real-Time Monitoring for Suspicious Activities, Developing and Testing Incident Response Plans, Assessing Security Practices of IoT Vendors, Providing User-Configurable Privacy[25] Settings, Ensuring Regulatory Compliance with Data Privacy Laws, Conducting Regular Security Audits and Assessments, Implementing Secure End-of-Life Processes for Devices, Segregating IoT Networks for Minimized Impact, Adopting Zero Trust Security Model, Collaborating with IoT Security Experts and Industry Groups for Threat Awareness and Best Practices.

4.4 Mitigation Strategies

The Mitigation strategies are essential for addressing vulnerabilities and enhancing the security of IoT systems across various layers and the protocols, the user may adopt this security approaches and monitor the IoT ecosystem to prevent from threats and vulnerabilities.

Generalized suggested strategies are implementing Message Integrity Checks for tampering detection, Implementing Role-Based Access Control (RBAC) for restricted user access, Implementing Robust Authentication Mechanisms,[27] Encrypting Data in Transit for traffic protection, Utilizing Public Key Infrastructure (PKI) for secure authentication, Implementing Rate Limiting to mitigate DoS attacks[18], Enforcing Input Validation to prevent SQL

injection and XSS attacks, Encrypting Sensitive Data both in transit and at rest, Employing Secure Communication Protocols[26] for data security, Ensuring Digitally Signed Firmware Up-dates for authenticity, Enforcing Strict Access Controls for devices and applications, Maintaining Regular Updates for machine learning models[20] and firm-ware, Implementing API Security Best Practices for secure APIs, Ensuring Secure WebSocket Implementation for communication security, Establishing Ethical Data Usage Guidelines for responsible practices, Implementing Strong Data Privacy Controls for user data protection, Conducting Regulatory Compliance Checks for adherence to data privacy regulations.

The layers such as Management and Monitoring uses (HTTP,MQTT) like protocols poses to Unauthorized Device Control manageable with possible mitigation like Secure device management, [24] an vulnerability such as Firmware Tampering, Unauthorized Access can be mitigate if uses mitigation strategies like Digitally signed firmware updates, Strong access controls.[9][14]

A User Interface Layer uses protocols such as (HTTP/HTTPS, WebSockets) is fronted towards the attacks such as Unauthorized Access, Data Leakage which can be mitigate using measures such as Strong authentication, [24] Data encryption, Input validation[9]

Regulatory Compliance layer which commonly uses the (HTTP/HTTPS,TLS/SSL) layer may front to attacks and breach things such as Data Breach, Regulatory Non-compliance can be mitigate in some extent using the strategies like Data privacy controls, Regulatory compliance checks[12][27], Ethical Violations Ethical data usage guidelines, Strong authentication[12][24][27].

The Table 2 is a study of various attack types and their associated concerns, including specific protocols that may be vulnerable. The table is a reference for understanding the landscape of cybersecurity threats and it consists of suggestions of possible solutions to security by mentioning mitigation strategies for each attack type, these strategies are for organizations and individuals with the knowledge needed to safeguard their digital assets and infrastructure effectively in once to focus on various layers of IoT from past different researches conducted.

Table 2. Layer (Protocol) wise Attack Vector table and Possible Mitigation.

Layer	Attack Vectors	Possible Mitigation Strategies
Sensors and Devices (MQTT, CoAP)	Data Tampering, Man-in-the-Middle	Message integrity checks, RBAC, Strong authentication [14]
	Unauthorized access, Device tampering.	Strong authentication, Physical security measures[9][14]
Connectivity (HTTP / HTTPS, DTLS)	Man-in-the-Middle, Eavesdropping	Use DTLS for secure communication, PKI for authentication[8]
	Packet Sniffing, Device Spoofing	Traffic encryption,[14] Strong authentication mechanisms.
Middleware (MQTT, AMQP)	Data Tampering, Man-in-the-Middle	Message integrity checks, RBAC, Secure communication [14]
	Message Spoofing, Unauthenticated Access	Role-based access control, Rate limiting[9][14]
Application (RESTful APIs, gRPC)	SQL Injection, Data Manipulation	Input validation, Data encryption, Strong Authentication [9][14]
	Algorithm Attacks, Unauthorized Access,	Access controls, Regular updates, Strong authentication, [8][14]
	API Exploitation, Data Leakage	API security measures, [14] Data encryption, Access controls
Integration (HTTP / HTTPS, WebSocket)	Man-in-the-Middle (MitM)	Secure WebSocket implementation, Encryption[14] [26]
Business (HTTP / HTTPS, MQTT)	Data Theft, Financial Data Breaches	Data access controls, [24] Encryption, Strong authentication

	Subscription Fraud	Strong user authentication, Access controls[9][14]
Security (TLS/SSL, OAuth)	Data Interception, Brute Force Attacks	Strong authentication, [4][9] Data encryption.[14]

4 CONCLUSIONS

The Internet of Things (IoT) has the potential to revolutionize industries, offering an increase in efficiency. However, this transformative power comes with significant security challenges. This comprehensive study shows depth layers of IoT architecture, vulnerabilities, communication protocols, potential threats and strategies to mitigate these security challenges. Furthermore, IoT architecture is multifaceted, consists of various layers, each with its unique functions and security considerations. In the study we have discussed about the various layers of IoT architecture and their demerits which leads to exploit protocols and attacks, in which we have discussed and proposed mitigation strategies to secure the future of IoT, users and organizations must adopt protective measures. These include implementing robust authentication, encrypting data during transit and storage, enforcing stringent access controls, ensuring regulatory compliance with an emphasis on transparency and user consent, prioritizing ethical data collection and usage, educating users and employees about IoT security risks, securing the future of IoT requires a forward approach that encompasses technological advancements, regulatory notes, ethical considerations and proactive security measures. By following these guidelines, users and organizations can harness the immense potential of IoT while safeguarding data privacy and security in an evolving digital landscape

ACKNOWLEDGEMENTS

REFERENCES

Ahmed J. Hintaw1 , Selvakumar Manickam1 , Shankar Karuppayah1 and Mohammed Faiz Aboalmaaly 2, "A Brief Review on MQTT's Security Issues within the Internet of Things (IoT)",Journal of Communications Vol. 14, No. 6, June 2019.

Abid, Muhammad, "IoT Security Challenges and Mitigations: An Introduction", Re-searchgate, Oct 2022.

Mourade Azrour , 1 Jamal Mabrouki , 2 Azidine Guezzaz , 3 and Ambrina Kanwal4 , " Internet of Things Security: Challenges and Key Issues", Hindawi Security and Com-munication Networks Volume 2021.

H.J. Felcia Bel, S. Sabeen, "A Survey on IoT Security: Attacks, Challenges and Coun-termeasures ", Webology, Volume 19, Number 1, January, 2022.

Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Se-curity: Application Areas, Security Threats and Solution Architectures," in IEEE Ac-cess, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

Rabbi, Md. Forhad et al. "Vulnerabilities to Internet of Things and Current State of the Art of Security Architecture." (2019).

A. Aldahmani, B. Ouni, T. Lestable and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures and Trends," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 281-292, 2023, doi: 10.1109/OJVT.2023.3234069.

A Murali M Rao Year: 2021 IoT: Security Issues and Challenges ICIDSSD EAI DOI: 10.4108/eai.27-2-2020.2303127 60

Rajmohan, T., Nguyen, P.H. & Ferry, N. A decade of research on patterns and architec-tures for IoT security. Cybersecurity 5, 2 (2022). https://doi.org/10.1186/s42400- 021-00104-7

O. Toutsop, S. Das and K. Kornegay, "Exploring The Security Issues in HomeBased IoT Devices Through Denial of Service Attacks," 2021 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communi-cations, Internet of People and Smart City Innovation (Smart-World/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 2021, pp. 407-415, doi: 10.1109/SWC50871.2021.00062.

Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity Threats, Countermeas-ures and Mitigation Techniques on the IoT: Future Research Directions. Electronics 2022, 11, 3330. https:// doi.org/10.3390/electronics11203330

Majid, A. (2023) Security and Privacy Concerns over IoT Devices Attacks in Smart Cit-ies (2022). Journal of

Computer and Communications, 11, 26-42. https://doi.org/10.4236/jcc.2023.111003

Ankit Dhatrak, Anshuman Sarkar; "Cyber Security Threats and Vulnerabilities in IoT" IRJET;Volume: 07 Issue: 03 — Mar 2020.

N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, At-tacks, Intrusion Detection and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

https://content.altexsoft.com/media/2020/08/iot-architecture-buildingblocks.png.webp

Khan, Muhammad Almas Khattak, Muazzam Jan, Sana Ullah Ahmad, Jawad Jamal, Sajjad Shaukat Shah, Awais Pitropakis, Nikolaos Buchanan, William. (2021). A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT. Sensors. 21. 10.3390/s21217016.

Y. al-Hadharni and F. K. Hussain, "DDoS attacks in IoT networks: A comprehensive systematic literature review," World Wide Web,Jan. 2021. 61

K. Doshi, Y. Yilmaz and S. Uludag, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," IEEE Trans. Dependable Secure Comput., early access, Jan. 8, 2021, doi: 10.1109/TDSC.2021.3049942.

S. E. Belanda, C. F. M. Foozy, A. Mustapha, P. S. S. Palaniapan and Z. Abdullah, "De-tecting botnet attack in Internet of Things (IoTs) environment by using machine learn-ing technique: A review," J. Crit. Rev., vol. 7, no. 8, 2020.

H. Wu, H. Han, X. Wang and S. Sun, "Research on artificial intelligence enhancing In-ternet of Things security: A survey," IEEE Access, vol. 8, 2020.

A. Munshi, N. A. Alqarni and N. A. Almalki, "DDOS attack on IoT devices," in Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), Mar. 2020,

C. V. Mart´ınez and B. Vogel-Heuser, "Towards industrial intrusion prevention sys-tems: A concept and implementation for reactive protection," Appl. Sci., vol. 8, no. 12,2018.

R. Panigrahi, S. Borah, A. K. Bhoi and P. K. Mallick, "Intrusion detection systems (IDS)—An overview with a generalized framework," Adv. Intell. Syst. Comput., vol. 1040

F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," IEEE Internet Things J., vol. 6, no. 5, Oct. 2019.

P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar and N. Kumar, "IoT vulnerability assessment for sustainable computing: Threats, current solutions and open challenges," IEEE Access, vol. 8, 2020.

Q.-D. Ngo, H.-T. Nguyen, L.-C. Nguyen and D.-H. Nguyen, "A survey of IoT malware and detection methods based on static features," Opt. Commun., 2020.

Carratù, M., Colace, F., Lorusso, A., Pietrosanto, A., Santaniello, D., Valentino, C. (2023). Data Mining Techniques for Intrusion Detection on the Internet of Things Field. International Conference on Cyber Security, Privacy and Networking (ICSPN 2022). ICSPN 2021Springer, Cham. https://doi.org/10.1007/978-3-031-22018-0_1

Ling, Z., Hao, Z.J.: Intrusion detection using normalized mutual information feature se-lection and parallel quantum genetic algorithm. Int. J. Semant. Web Inf. Syst. (IJSWIS) 18(1), 1-24 (2022).

Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. 84 (2017). https://doi.org/10.1016/j.jnca.2017.02.009.

ARNAR PÉTURSSON, Ethical Hacking of a Ring Doorbell, https://www.diva-portal.org/smash/get/diva2:1751192/FULLTEXT01.pdf

Xu, Yuan & Han, Xingshuo & Deng, Gelei & Li, Guanlin & Liu, Yang & Li, Jiwei & Zhang, Tianwei. (2022). SoK: Rethinking Sensor Spoofing Attacks against Robotic Ve-hicles from a Systematic View.

Verkada Security Incident Report : https://docs.verkada.com/docs/Security_Incident_Report_Version1.2.pdf

Vakhshiteh, Fatemeh & Nickabadi, Ahmad & Ramachandra, Raghavendra. (2021). Adversarial Attacks Against Face Recognition: A Comprehensive Study. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3092646.

Peloton's API exposes riders' private data. https://www.securitymagazine.com/articles/95146-pelotons-api-exposes-riders-private-data.