www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 13 Issue 02 February 2024, Page No. 26001-26006
ISSN: 2319-7242 DOI: 10.18535/ijecs/v13i01.4788

A Secure Authentication mechanism for accessing IoT devices through Mobile App

Parvinder Kaur[1], Heena Arora[2]
Research Scholar[1] ,Assistant Professor[2]
Universal Group of Colleges, PTU, Lalru, Punjab, India

Abstract

In today's digital era, IoT devices have become vital for connecting things to the internet, allowing users to control them remotely from anywhere. The primary advantage of using IoT devices lies in the ability to save time and access resources remotely. However, with the increasing use of IoT devices, there are growing challenges related to security and privacy. Key aspects of IoT security include authentication, confidentiality, and integrity, which are essential for a robust security mechanism.While current IoT protocols offer varying levels of security, it has become crucial to defend against different types of attacks like masquerade attacks, man-in-the-middle attacks, replay attacks, password guessing, impounder attacks, and Denial of Service (DoS) attacks. In this paper, we analyze the security of IoT devices and propose a smart solution. We employ a temperature sensor (DHT22) with NodeMCU to transmit data through the IoT protocol and receive it on a mobile device. We assess how data is securely transmitted from IoT devices to mobile devices, highlighting challenges faced during prototype development. Moreover, we emphasize the security level in transmitting data from IoT devices to the cloud and from the cloud to mobile devices, presenting a prototype capable of securely and seamlessly transmitting data to the cloud.

Keywords—IoT, security, Authentication, SSL, IoT devices, IoT Mobile Application.

1. Introduction

Nowadays IoT is a fast growing technology and almost all domain experts believe that IoT will be integrated with all aspects and demand will increase rapidly during this period [1].

The Internet of Things (IoT) is a connected world where smart devices can operate and control other devices through IoT technology, which relies on the internet. With more IoT devices, people can experience more convenience and save more time. In cases where internet access is limited, LoRa devices can pass data up to 5 km without internet connectivity, providing an advancement in connectivity for IoT devices in remote or inaccessible areas. However, as the IoT industry grows, it faces challenges in areas such as security, data collection, unauthorized access, data manipulation, network penetration, eavesdropping, and IoT firmware updates. Experts have implemented various protocols and technology upgrades to address these challenges. Additionally, IoT devices are increasingly integrating with AI to become more intelligent and powerful.IoT technology plays a significant role in scenarios where humans operate or monitor from specific locations, enabling remote control of machines. As the world transitions from 4G to 5G networks, the demand, production, and usage of IoT are poised to increase significantly, propelling advancements in IoT technologies and the industry overall. The hardware industry's high-level AI-based integrated circuits will enhance edge-level data processing, handling, and AI operations' efficiency. The adoption of IoT devices in smart homes and cities will contribute to enhanced efficiency and convenience, elevating the lifestyle of the smart society and conserving resources. Furthermore, industries stand to gain increased profits through the integration of IoT technologies.

Security emerges as a crucial aspect in the utilization of IoT devices, an aspect often overlooked by consumers. Many are unaware of potential security issues, as IoT device manufacturers tend to neglect adopting security compliance guidelines, such as OWASP, for cost-effectiveness reasons. Adhering to recommended guidelines and establishing secure connections is vital to minimize the risk of data breaches or hacking incidents involving these devices.

The paper is organized as follows: Section two reviews related work in the field of IoT security & Privacy. Section three outlines the proposed model, and Section four presents the experiment analysis. The final section offers a summary of the research in the form of a conclusion, including insights into future work.

1. RELATED Work

A. Internet of Things (IoT)

The Internet of Things (IoT) links physical devices, like vehicles and buildings, embedding them with electronics, sensors, and connectivity to collect and share data. This technology has transformative potential, enabling seamless communication between objects and people. IoT's key advantage lies in its capacity to gather diverse data from sensors, cameras, and other devices, providing insights for informed decision-making. In healthcare, IoT devices like fitness trackers offer remote health monitoring. Industrial automation benefits from IoT by optimizing production processes, reducing downtime, and increasing efficiency. In transportation, IoT optimizes logistics and improves traffic flow. In smart cities, IoT enhances public services, reduces environmental impact, and boosts overall quality of life. Despite its positive impact, concerns about security and privacy arise as IoT collects personal data. Ensuring data protection and integrating security throughout the development process is crucial. While IoT holds immense potential to reshape our lives and industries, addressing security and privacy concerns is paramount.

B. *Security Challenges*

The Internet of Things (IoT) could transform our daily lives by enabling objects to communicate with each other and us. Yet, as IoT gains widespread adoption, security and privacy concerns arise. IoT devices are susceptible to cyber attacks, posing risks to individuals, organizations, and society. Security challenges stem from devices often lacking design with security in mind due to limited processing power and memory. Many lack user interfaces, complicating tasks like password changes. Standardization issues further hinder security, making it challenging to ensure device security and communication. IoT devices can serve as entry points for cyber attackers, compromising network security. Additionally, the remote deployment of IoT devices limits visibility and control, making it challenging to detect and respond to security threats promptly. To tackle these challenges, a holistic approach to IoT security is crucial. This involves integrating security into the entire product development process, employing measures like encryption and firewalls, and ensuring regular updates to safeguard against vulnerabilities. In conclusion, while IoT holds transformative potential, addressing these security challenges is essential for its secure and safe deployment.

C. *Communication Protocols*

The Internet of Things (IoT) is a network of physical devices embedded with electronics, software, sensors, and connectivity, enabling them to collect and exchange data. To facilitate communication and data exchange, these devices rely on communication protocols—rules and standards governing information exchange. TCP/IP, or Transmission Control Protocol/Internet Protocol, is a widely used IoT communication protocol for routing data packets over the internet, serving applications like web browsing and email. MQTT, or Message Queue Telemetry Transport, is a lightweight protocol designed for low-power devices and networks with limited bandwidth, commonly used in sensor networks and machine-to-machine communications. Bluetooth, a wireless technology, facilitates short-distance communication in wearables, smart home devices, and industrial automation. Zigbee, a low-power and low-data-rate protocol, suits devices with limited power, commonly used in smart home devices, building automation, and industrial control systems. LoRaWAN, or Long Range Wide Area Network, supports long-range communications for applications like smart cities and agriculture. Other protocols, including Zigbee, Z-Wave, CoAP, DDS, and AMQP, find applications in various fields. Adopting standard communication protocols ensures interoperability and scalability in IoT systems. The choice of a protocol depends on application requirements, considering factors such as data type, range, power, and cost constraints. As IoT technology advances, new protocols will emerge to meet evolving application needs.

D. *IoT security vs traditional IT security*

The Internet of Things (IoT) has transformative potential, allowing everyday objects to communicate. However, as IoT adoption grows, security considerations become crucial. Unlike traditional IT security, IoT security faces challenges due to the diverse array of devices, ranging from simple sensors to complex industrial machines. These devices vary in capabilities and vulnerabilities, complicating security measures. Many IoT devices are small, low-power, and have limited resources, making traditional security measures challenging to implement. The lack of standardization in devices, platforms, and protocols further complicates security, making it challenging for professionals to protect against threats. IoT devices can pose risks to network security, serving as entry points for cyber attackers. Additionally, the remote deployment of IoT devices hampers visibility and control, making it challenging to identify and respond to security threats promptly.

2. Proposed Model

Our paper proposes a model integrating IoT devices with mobile platforms for temperature monitoring applications. Unlike traditional online platforms, our model directly connects IoT devices with mobile apps, offering simplicity and efficiency. We've established our server to respond consistently in a Pub/Sub manner, allowing users to remotely update device configurations by changing topics. The application, currently in beta, provides users with significant benefits, as illustrated in the figures.

For hardware, we utilize the ESP8266 microcontroller and DHT22 temperature sensor, known for its accuracy in measuring temperature and humidity. Our prototypes focus on understanding IoT application security and communication. Software-wise, we've developed a mobile application enabling seamless integration of devices with essential parameters. Data is stored locally in the mobile device, accessible in Excel format for analysis. We employ the MQTT protocol, renowned for its efficiency in IoT applications, ensuring swift and reliable data transmission. The Publish/Subscribe protocol facilitates seamless communication between multiple subscribers and publishers.

The mobile application displays live IoT device data, with color-coded indicators for upper and lower thresholds, along with the current value

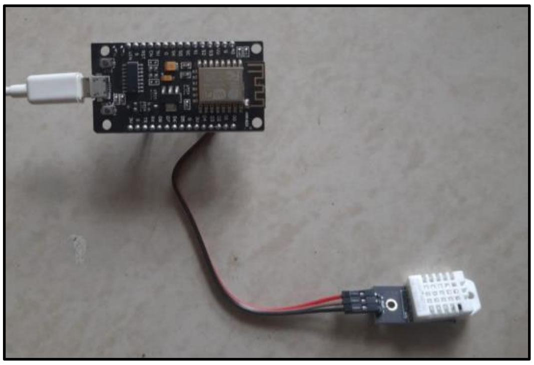

Figure1: Prototype of IoT device

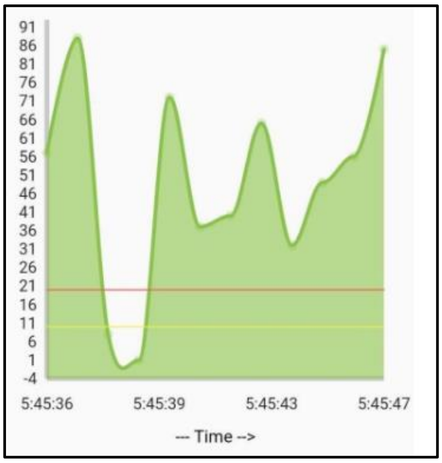

Figure2: Mobile Application shows Live Temperature

3. Experiment Analysis

With IoT, accessing live data remotely is our primary goal, aiming for secure, smooth, and portable usability. Our well-tested prototype ensures functionality in diverse environments. Using the more accurate DHT22 for experiments, we observed secure data transmission with minimal errors. Testing various attacks, including brute force, DoS, and Man-in-the-Middle, revealed negligible possibilities of breaches. Employing additional parameters like SSL security and encrypted topic names enhanced authentication and authorization levels, significantly reducing the chances of attacks. We conclude that implementing proper security measures at the device end renders security breaches negligible.

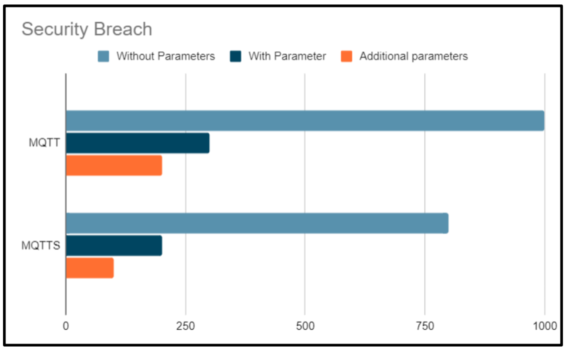

Figure 3: Security breach analysis on IoT devices

4. Conclusion

The IoT domain stands as a prominent force, poised to revolutionize industries, streamline operations, and facilitate instant connectivity worldwide. Our research, centered on ensuring the security of IoT devices and the secure transmission of data to mobile applications, utilized the precise DHT22 for ambient temperature capture. We emphasize the development of secure connections between smart IoT devices, servers, and mobiles to ensure seamless and secure operations. The creation of a dedicated mobile app serves as an optimal means for connecting any IoT device. As we delve into security and privacy considerations, our stringent measures thwart potential threats like man-in-the-middle attacks, DoS attacks, tampering, and jamming. To further enhance IoT connectivity, standardized guidelines are imperative, enabling the seamless interconnection of diverse devices, protocols, and applications.

Looking ahead, we envision the integration of AI to provide users with early notifications regarding temperature changes. The ongoing commitment involves developing multiple prototypes and platforms, empowering users to harness IoT technology effectively.

Acknowledge:
I extend my sincere gratitude to my mentors, **Heena Arora** and **Vijay Paul Singh,** for their invaluable guidance and support throughout the research process. Their expertise and encouragement have been instrumental in shaping the direction and outcomes of this paper.

References

1. Ray, Partha Pratim. "A survey of IoT cloud platforms." *Future Computing and Informatics Journal* 1.1-2 (2016): 35-46.
2. Gaitan, Nicoleta Cristina. "A long-distance communication architecture for medical devices based on LoRaWAN protocol." Electronics 10.8 (2021): 940.
3. Shah, Rushabh, and Alina Chircu. "IOT and ai in healthcare: A systematic literature review." Issues in Information Systems 19.3 (2018).
4. Samie, Farzad, Lars Bauer, and Jörg Henkel. "IoT technologies for embedded computing: A survey." *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*. IEEE, 2016.
5. Lee, Suk Kyu, Mungyu Bae, and Hwangnam Kim. "Future of IoT networks: A survey." *Applied Sciences* 7.10 (2017): 1072.
6. Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." *Computer networks* 148 (2019): 283-294.
7. Ishaq, Isam, et al. "IETF standardization in the field of the internet of things (IoT): a survey." *Journal of Sensor and Actuator Networks* 2.2 (2013): 235-287.
8. Gilchrist, Alasdair. *IoT security issues*. Walter de Gruyter GmbH & Co KG, 2017.
9. Shah, Sajjad Hussain, and Ilyas Yaqoob. "A survey: Internet of Things (IOT) technologies, applications and challenges." *2016 IEEE Smart Energy Grid Engineering (SEGE)*. IEEE, 2016.
10. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017.
11. Schurgot, Mary R., David A. Shinberg, and Lloyd G. Greenwald. "Experiments with security and privacy in IoT networks." *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2015.
12. Safdar, Noreen, Hala Asif, and Fatima Farooq. "Energy Use and Human Health Nexus in Pakistan." *Review of Economics and Development Studies* 6.3 (2020): 661-674.
13. Gravely, Shannon, et al. "Discussions between health professionals and smokers about nicotine vaping products: Results from the 2016 ITC Four Country Smoking and Vaping Survey." *Addiction* 114 (2019): 71-85.
14. Abu-Elkheir, Mervat, Mohammad Hayajneh, and Najah Abu Ali. "Data management for

the internet of things: Design primitives and solution." *Sensors* 13.11 (2013): 15582-15612.

15. Bohli, Jens-Matthias, et al. "SMARTIE project: Secure IoT data management for smart cities." *2015 International Conference on Recent Advances in Internet of Things (RIoT)*. IEEE, 2015.
16. Zhang, PeiYun, MengChu Zhou, and Giancarlo Fortino. "Security and trust issues in fog computing: A survey." *Future Generation Computer Systems* 88 (2018): 16-27.
17. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.
18. Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." *Computer* 50.2 (2017): 76-79.
19. Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." *Internet of Things* 5 (2019): 41-70.
20. Ramotsoela, Daniel, Adnan Abu-Mahfouz, and Gerhard Hancke. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study." *Sensors* 18.8 (2018): 2491.
21. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." *2014 international conference on privacy and security in mobile systems (PRISMS)*. IEEE, 2014.
22. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.
23. Cerullo, Gianfranco, et al. "Iot and sensor networks security." *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*. Academic Press, 2018. 77-101.
24. Tang, Xiao, Pinyi Ren, and Zhu Han. "Jamming mitigation via hierarchical security game for iot communications." *IEEE Access* 6 (2018): 5766-5779.
25. Thakkar, Ankit, and Ritika Lohiya. "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." Archives of Computational Methods in Engineering 28.4 (2021): 3211-3243.
26. Lin, Yun-Wei, Yi-Bing Lin, and Chun-You Liu. "AItalk: a tutorial to implement AI as IoT devices." IET Networks 8.3 (2019): 195-202.