Title Of The Paper

A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures

Paper Link

https://ieeexplore.ieee.org/document/8742551

1. Summary

1.1. Hypothesis

The paper discusses the significance of the Internet of Things (IoT) as the next era of communication, enabling physical objects to seamlessly create, receive, and exchange data. The security challenges and sources of threats in IoT applications are thoroughly reviewed, including issues like privacy, authentication, management, and information storage. The authors have introduced four technologies such as blockchain, fog computing, edge computing, and machine learning as potential solutions to enhance security in IoT.

1.2. Contribution

The authors have assessed open issues, challenges, and outlined future research directions in the realm of developing secure IoT applications. A detailed explanation is offered for various threat sources present in different layers of the IoT ecosystem. This includes identifying potential security risks in sensors and actuators, communication networks, middleware, and end-to-end applications.

1.3. Methodology

Some of the most popular IoT applications which are discussed in this paper are Smart Cities, Smart Environment, Smart Metering and Grids, Security and Emergencies, Smart Retail, Smart Agriculture and animal farming and Home automation which all lack security in four building layers. Further in sensing layer the common vulnerabilities are Node capturing, Malicious Code Injection Attack, False Data injection Attack. Access attack, DoS attack, Data transit attack are some common security issues in Network layer. In middleware layer Man in the Middle attack and SQL Injection attack, also in application layer Data thefts, Service Interruption attacks are most prominent. The authors have suggested Blockchain as a strong, tamper-proof, distributed, and open data structure for IoT data, supported by features like miners' competition, anonymity, and cryptographic hash keys. Moreover Blockchain is seen as preventing data loss, spoofing attacks, and unauthorized access. Next, fog computing is introduced, complementing cloud computing by handling IoT data locally for better management. The paper presents two frameworks: Fog-Device, where fog nodes provide services without involving cloud servers, and Fog-Cloud-Device, where simple decisions are made at the fog layer, and complex decisions at the cloud layer which can be able to handle unauthorized access and ensure data integrity.Fog computing uses public and private keys for communication, allowing only intended parties to access encrypted data, thus addressing security issues faced by IoT applications. In addition, protection against spoofing attacks involves ML techniques such as Q-learning, Dyna-Q, Support Vector Machines (SVM), Deep Neural Network (DNN) model, incremental aggregated gradient (IAG), and distributed FrankWolfe (dFW).

These techniques not only enhance detection and classification accuracy but also reduce error rates and false alarm rates. Additionally, a particle swarm optimization and backpropagation algorithm for MLP training enhances wireless network security against DoS attacks. Lastly, edge computing is added which allows organizations to keep data within their borders. This is particularly relevant in regions with strict regulatory acts like GDPR.

1.4.Conclusion

This paper delves into open issues and challenges stemming from these solutions. It offers insights into the state-of-the-art in IoT security and outlines future research directions aimed at enhancing security levels in IoT. The presented survey is anticipated to be a valuable resource for improving security in upcoming IoT applications.

2. Limitations

2.1. First Limitation

Though there are many benefits of integrating Blockchain in IoT applications, it lacks in handling the garbage data. Numerous instances of invalid data, such as addresses associated with obsolete smart contracts, persist without deletion. This negatively impacts the overall application's performance, highlighting the necessity for more effective methods to manage and dispose of garbage data within the blockchain.

2.2. Second Limitation

While edge computing offers numerous advantages for enhancing the security and performance of IoT applications, there are significant challenges associated with relying solely on the edge layer for all computations. Edge devices, encompassing sensors, RFID devices, actuators, tags, and embedded devices, are vulnerable to attacks, and a compromise in the edge layer could endanger the entire IoT system. Specific issues related to edge devices involve sleep deprivation attacks, battery draining attacks, and outage attacks, particularly impactful given the resource constraints of these devices, primarily their reliance on battery backup. Striking the right balance between storing and processing data on the edge or cloud is crucial, as overwhelming edge devices with excessive data may adversely affect the entire application.

3. Synthesis

In the future, blockchain can be expected to continue playing a crucial role in securing IoT devices and data. Its decentralized and tamper-proof nature provides robust protection against cyber threats. Also continued efforts to improve the scalability of fog computing architectures, enabling them to handle the increasing volume of IoT devices and data. Additionally, edge computing can facilitate the development of more autonomous and self-sufficient IoT devices by handling complex computations locally.