Module 9: Activity 6

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

October 21, 2023

Securing the Internet of Things:

Fog Computing's Role in Mitigating IoT Security and Privacy Challenges

Introduction

The Internet of Things (IoT) has developed into a cutting-edge, never-ending network of gadgets and sensors that offers a variety of services. IoT device adoption is expanding, though, which poses questions about security and privacy. Because IoT devices usually have constrained resources, securing data, maintaining user privacy, and defending against attacks offer particular challenges. This article will discuss the security and privacy risks in the IoT ecosystem and offer the idea of using the cloud as a contract to allay these worries.

Fog computing, often referred to as networked cloud computing, offers an IoT device platform that may boost security, lower latency, and enhance data processing. Due to its support and location data, cloud computing not only creates new security and privacy concerns, but also new difficulties. In-depth analysis of these issues is provided in this article, with an emphasis on the role that cloud computing plays in bolstering security measures for IoT applications.

Additionally, this study offers proof that data transport may be used effectively in Internet of Things applications. Due to the constrained usage and connectivity of IoT devices, existing methods of certificate revocation, such as the Certificate Revocation List (CRL) and Online Certificate Services (OCSP), have restrictions. In order to limit tiny print, lower connection costs, and provide instantaneous updates in the Internet of Things, the study advocates using the cloud to manage certifications.

Concepts

This work discusses a wide range of interrelated concepts that are essential to understanding how security, privacy, the Internet of Things, and cloud computing have come together. The Internet of Things (IoT) is a vast network of linked objects that exchange data over the Internet, changing many facets of how we gather, examine, and utilize data. These Internet of Things (IoT) devices usually have limitations, such scarce resources, which raises security and privacy issues.

Fog computing, a development of cloud computing, is the main topic of discussion. It involves moving computer and data processing capability closer to the network's edge, reducing latency, lengthening the time it takes to analyze data, and adapting it for Internet of Things applications. It represents a fundamental shift in the IoT ecosystem's approach to data processing. Certificate Revocation Schemes, a cornerstone of digital security, emerge as a key topic. The article explores two prominent approaches, Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP). CRLs are files that list revoked certificates' serial numbers, while OCSP allows clients to verify a certificate's real-time status, and both play a crucial role in ensuring secure communications and data integrity in IoT.

In the context of resource-optimized IoT devices, another important concept is introduced. It is difficult to offer effective security because of its low power consumption, bandwidth, storage, and battery life. The necessity to secure IoT users and data sources was stressed during discussions on communication overhead, unnecessary data changes during communication management, and privacy. Access control is yet another crucial concept in determining who has access to what resources. In the IoT ecosystem, access control is increasingly important, especially for IoT devices and data. Signed or unofficial intrusion detection systems are needed in the IoT ecosystem to monitor and detect potential security issues. It emphasizes the efficient design of security solutions to address specific IoT concerns like energy efficiency and resilience.

The article seeks to assess how the combination of these components and the use of the cloud may be able to address the security and speed privacy issues in the IoT environment. It is a prime example of the ability to create integrated, effective, and safe ecosystems by combining cloud computing, IoT devices, and cloud computing. These concepts are inextricably linked and provide the framework for the challenging problem-solving approaches described in this article. There are a number of security threats and concerns in the IoT ecosystem. The ongoing expansion and promise of the Internet of Things while safeguarding private information depends on the integration of these concepts.

Facts and Statistics

The relevance of addressing security and privacy issues in the context of IoT and cloud computing is demonstrated by facts and numbers. IoT device use reached 2.6 million in 2016, up 30% from the previous year, according to Gartner projections. The fast growth of IoT devices and the enormous amount of data they produce, which poses major security and privacy issues, are highlighted in this article. De-identification is urgently needed and effective, as shown by the fact that over 30% of testimonies were retracted within the first two days of publication, per one study. These statistics highlight both the widespread usage of IoT devices and the urgent need for solutions to security and privacy issues in order to protect private users' data and the integrity of the IoT ecosystem. This article also looks at the typical response time for Online Credential Presence Protocol (OCSP) responders, which shows that it is 291 milliseconds on average. It displays the lag time for real-time verification. These numbers highlight how challenging it is to provide reliable and effective IoT connection.

The article also covers big data and transmission overhead. It shows the amount and update time of certificate revocation list (CRL) records for all certificate authorities (CAs) involved in Alexa's TLS handshake for over 1 million record names. These numbers show that CRL archive sizes range from 793 bytes to 5 Mb, and that updates span anywhere between a few days to a year. This data highlights the challenges of managing CRLs for

various CAs by showing a wide variety of CRL duration and update frequency. In the context of communication payload, this article evaluates the packet sizes of various extraction techniques. According to the amount of certificates removed, it calculates the CRL and OCSP packet sizes and discovers a sizable difference between these and cloud-based approaches. In order to increase IoT connection, this research demonstrates the potential effectiveness of cloud computing implementation by reducing communication overhead and bandwidth usage.

The concept of fog computing, which extends cloud capabilities to the network edge, is introduced in the article, and its potential advantages for IoT systems are highlighted. It demonstrates how real-time requirements, which are essential in most IoT applications, are met by fog computing and how this aligns with the need for speedy processing of data provided by various IoT devices. Because of the fundamentally challenging characteristics of the Internet of Things, such as its constrained processing power, bandwidth, battery life, and storage capacity, standard cloud computing is unable to meet real-time requirements. Understanding the limitations of cloud computing and the suitability of fog computing, particularly for IoT applications, depends critically on this background.

The article’s discussion of vulnerability identification is another crucial component. As a result, malicious IoT nodes pose as trustworthy nodes to get or exchange data for illicit purposes. It highlights the importance of solving this issue and discusses work by Liran Ma and others that proposes a hybrid technique for identifying malicious information on Wi-Fi-based connections. This idea highlights the need of data protection while also highlighting potential threats in the IoT ecosystem. It also acts as a reminder of the necessity of security precautions.

In the IoT environment, privacy issues are also covered in the article. It talks about user data leakage and how it affects the research community, focusing on data, location, and data consumption. It highlights the necessity of protecting users' sensitive data and presents possible privacy protection solutions for a variety of IoT applications. These decisions add another layer to the larger conversation about security and privacy in the

context of IoT by demonstrating the necessity for privacy measures given the IoT's rapid expansion and the data it creates to safeguard users' sensitive information.

The facts and data given in this article highlight the significance and difficulty of IoT security and privacy issues. They provide context for solutions and stress the necessity of creating efficient, timely procedures to deal with these problems, particularly those pertaining to the expensive IoT device set. The report also shows that IoT is expanding, as seen by an increase in IoT devices and data collection, and that security and privacy issues need to be addressed.

Summary and Conclusions

In this article, the authors look at how the dynamic area of cloud computing might be used as a transformational approach to bridge the gap between cloud data centers and Internet of Things (IoT) devices. The essential benefits of cloud computing—such as reduced latency, improved security, lower bandwidth usage, location awareness, scalability, and regional reach—are emphasized by the writers. They believe that these qualities make them ideal for meeting the demanding needs of real-time IoT applications, which demand rapid decision-making and low-latency data access..

However, this article is careful to point out that there are several security and privacy problems associated with the expansion of IoT devices. The issues include those with authentication, trust, vulnerability detection, privacy, access control, data access, and data security. The main topic of discussion is how authentication data is disseminated in the context of the Internet of Things. In the resource-constrained IoT, the authors show the shortcomings of two popular techniques, the Revocation List (CRL) and the Online Certificate Process (OCSP). They suggested Bloom filtering and a brand-new decertification process built on cloud computing to deal with this problem. This ground-breaking method aims to improve flexibility, eliminate communication overhead, and decrease storage requirements, all of which will lead to increased security for the IoT ecosystem.

The importance of research on IoT and cloud computing security and privacy is also emphasized in the article. Privacy protection, security and effectiveness, authentication, attacks, location verification, and access control are only a few of the research-related issues that haven't been fully addressed. These study questions underline the rising importance of IoT security and privacy and the crucial role that cloud computing will play in ensuring its efficiency, safety, and privacy. Implementing cloud computing is a crucial step in ensuring the dependability and longevity of IoT applications in a world where IoT devices are becoming more widely used.

The critical necessity to address security and privacy issues in the expanding IoT environment is further emphasized by this work. The importance of using the cloud as a tool to address these issues is emphasized, as are its unique characteristics as an IoT security solution. The decertification procedure confirms the dedication to improving IoT device performance while safeguarding the security and privacy of these systems.

References

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (Year). Fog Computing for the Internet of Things: Security and Privacy Issues. George Washington University.