Chapter 15
Security in Internet of Things Applications Using Network-Attached Storage for Resource Usage Optimization

Antony Taurshia
https://orcid.org/0000-0001-9129-1859
Division of Data Science and Cyber Security, Karunya Institute of Technology and Sciences, Coimbatore, India

D. Ponmary Pushpa Latha
https://orcid.org/0000-0003-4000-0294
Division of Digital Sciences, Karunya Institute of Technology and Sciences (Deemed), Coimbatore, India

S. Princy Suganthi Bai
Department of MCA, Hindustan Institute of Technology and Science, (Deemed), Coimbatore, India

R. Vignesh
https://orcid.org/0009-0006-6065-987X
Division of Digital Sciences, Karunya Institute of Technology and Sciences (Deemed), Coimbatore, India

D. Joseph Pushpa Raj
https://orcid.org/0009-0006-6033-9825
Department of Computer Science and Engineering, PSN College of Engineering and Technology, Tirunelveli, India

DOI: 10.4018/979-8-3693-5448-3.ch015

ABSTRACT

The Internet of Things (IoT) enhances human society by enabling common objects to access the internet and make insightful conclusions, using technology elements like RFID, sensors, embedded devices, and service platforms. The IoT is enabled by certain elements, but they have limitations due to their limited processing power and resource availability. The constraints in IoT applications can compromise the security primitives that are fully utilized. The recommended method utilizes Network Attached Storage (NAS) to encrypt data before it leaves the local network, minimizing the strain on devices with limited capabilities. Cloud service platforms can be eliminated by securing data locally on the enterprise premises, eliminating the need for cloud-based services.

INTRODUCTION

The combination of physical objects or devices with sensors, software, and connectivity that allows them to share data with other devices or systems over the Internet is referred to as the Internet of Things IoT (Lin et al., 2017). It allows for the seamless interaction of multiple wearables and devices to create an interconnected ecosystem that can perform complex tasks with minimal human intervention IoT work using information provided by devices that together it brings real-time collection and analysis, enabling businesses and individuals to make data-driven decisions (Lin et al., 2017).

However, the IoT presents major challenges, such as security and privacy concerns, standards issues, and complex data management. IoT devices have different positions in consumer products Laptops, desktops, and smartphones connected to IoT applications can adopt more secure cryptographic primitives. Embedded systems with limited resources can accommodate tolerable cryptography. RFID tags and high-capacity sensor nodes can only accept hardware-based cryptographic primitives. Despite these challenges, IoT continues to grow rapidly, with estimates suggesting that by 2027 more than 41 billion IoT devices will be connected (Wang et al., 2022).

With the increasing data dependency and the growing concern for data security, individuals and organizations face the challenge of finding a storage solution that balances accessibility, security, and affordability. Cloud storage services offer convenience and remote access but raise concerns about data privacy and security (Cao et al., 2020). Therefore, there is a need for an alternative solution that combines the benefits of cloud storage, local control, and enhanced security while remaining cost-effective(Wang et al., 2022).

FaceTimeMap: Multi-Level Bitmap Index for Temporal Querying of Faces in Videos

Buddha Shrestha, Haeyong Chungand Ramazan S. Aygün (2019). *International Journal of Multimedia Data Engineering and Management (pp. 37-59).*
www.irma-international.org/article/facetimemap/233863