Chapter 35
A Cloud-Assisted Proxy Re-Encryption Scheme for Efficient Data Sharing Across IoT Systems

Muthukumaran V.
VIT University, India

Ezhilmaran D.
VIT University, India

ABSTRACT

In recent years, the growth of IoT applications is rapid in nature and widespread across several domains. This tremendous growth of IoT applications leads to various security and privacy concerns. The existing security algorithms fail to provide improved security features across IoT devices due to its resource constrained nature (inability to handle a huge amount of data). In this context, the authors propose a cloud-assisted proxy re-encryption scheme for efficient data sharing across IoT systems. The proposed approach solves the root extraction problem using near-ring. This improves the security measures of the system. The security analysis of the proposed approach states that it provides improved security with lesser computational overheads.

INTRODUCTION

The term Internet of things (IoT) is defined as a network through which the data is collected, processed and analyzed to provide various services using a series of interconnected devices (Zhou et al., 2017 & Abomhara et al., 2014). The growing adoption of IoT techniques makes its application prevalent across various domains, especially with real-life applications. Some of the major applications of IoT system include smart homes, smart cities, transportation, industrial manufacturing, underwater resource management, and healthcare systems. The data generated from the IoT applications are highly voluminous,

DOI: 10.4018/978-1-6684-7132-6.ch035

which the existing IoT devices fail to store and process. This is due to the resource constrained nature of the IoT devices. That is IoT devices possess limited storage and computational capabilities so that it fails to store and process highly voluminous sensor data at real-time. Due to this motive, the IoT devices are integrated with effective middleware's such as cloud computing to outsource storage and computation processes. That is the data collected from IoT devices are stored across the cloud computing infrastructures for further processing and decision-making purposes. In general, IoT devices make use of cloud-based infrastructure (IaaS) services, as it does not only require data storage facilities but also need efficient data processing and computation capabilities (Tao et al., 2014 & Qu et al., 2016). This creates the requirement of efficient security mechanisms for secure management of cloud based IoT systems.

Cloud computing is a unique paradigm offering a wide variety of services across the internet through a series of interconnected computing resources (Youseff et al., 2008). It enables one to store and access confidential data across the internet instead of their local system setups. The NIST definition of cloud computing states that Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Tsai et al., 2010). In other words, the term cloud computing offers on-demand network access services that can be used from anywhere and at any time. The on-demand self-service, broad network access, resource pooling, rapid elasticity, measured services are the key features of the cloud computing systems.

Software as a Service (SaaS), Platform as s Service (PaaS) and Infrastructure as a Service (IaaS) are the three major services provided by the cloud computing systems. The term SaaS offers software services to the cloud users. NetSuite and Salesforce customer relationship management (CRM) are the some of the examples of SaaS. PaaS enables the cloud users to run their applications across cloud computing platforms without the use of their local system setup. Google App Engine and App Stratos are the examples of SaaS. Infrastructure services (IaaS) is otherwise known as Everything as a Service or Hardware as a Service. In IaaS a complete computing platform made up of virtual machines connected to a network is given to the users. Virtual machine (VM) is a software program or an operating system that forms the concept of the IaaS systems. In simple terms, a virtual machine is a guest created from the host machine (another computing environment). A single host can contain multiple virtual machines at a single point of time. Windows Azure and Amazon EC2, Google Compute Engine (GCE) are the best examples of IaaS (JoSEP et al., 2010).

In IaaS, the end users log into the dashboard and raise VM requests. Whenever the cloud server receives the VM request it decides the hypervisor nodes and creates the virtual machine. A virtual machine is configured with the user- defined CPU and storage specifications. Upon the successful creation of the virtual machines, the end users make use of the cloud infrastructure services for an infinite period of time. SaaS and PaaS offer users with the static services to the system users with specified time limits. This dynamic nature of the IaaS services creates the development of high performance and permanent availability measures across the cloud computing environment (Zhang et al., 2010). Thus, the use of proxy re-encryption techniques can reduce the end user overheads and provides improved services to the cloud users.

As, the power of cloud server is finite and the capability of IoT devices are resource constrained in nature. The integration of cloud and IoT systems provide better solution to manage growing amount of IoT device data. In today's world, the applications of IoT is widespread and it ranges from personal data to data sensed from a particular application environment. In such cases, the attacker can easily collect the