The Implementation Results of Identity-Based Hashing Algorithm for Iot

Rafidha Rehiman K A, S Veni

Abstract—Nonrepudiation in Mobile environment is a major challenge in the area of IoT security. Public-key-based Digital Signature schemes are common and their computational requirements and complexities do not support constrained devices. This paper presents the design and implementation results of light weight nonrepudiation architecture based on public key cryptography and Elliptic Curve addition to reduce the overhead of processing and communication.

Keywords—Nonrepudiation, Digital Signature, IoT Security, ECC cryptosystem, Hashing

I. INTRODUCTION

Internet of Things (IoT) is an important technological advancement, which enables communication between all types of things including living beings. In IoT we can control everything with the help of software including human body parts. IoT changes every aspect of life like Education, Communication, Research and Science, Government function, Business and Human behavior (humanity) [1].

The communication language of IoT is a heterogeneous interoperable protocol and many different types of devices communicate with one another. The IoT devices exchange a wide variety of vast information. IoT brings enough challenges, as these devices continuously collect a vast amount of private information. Also, heterogeneous connections are not scalable. Unlike user-operated computing devices smart things with sensors and actuators are not properly controlled when connected to the Internet.

The IoT devices sporadically establish connection with other devices and communication entities connected to the network. There is a need in IoT environment to prevent some devices from accessing certain services and restrict the communication.

One major challenge faced by IoT is the problem of securing the network [2], its associated resources and its reliability issues. It has the right in the environment as server to know who are negotiating and accessing the information. Revelation of the sensitive information to unauthorized consumers may lead to security problems in an organization.

The very first step that needs to be taken care of to ensure the integrity and nonrepudiation is hardening the device against the intrusion into the secure perimeter [3]. For the IoT infrastructure, we need to implement the solutions which use minimum resources and communication power. Also, the access control models are a must to prevent policy violation in an Organization.

Revised Manuscript Received on September 06, 2019

Rafidha Rehiman K A, department of Computer Science, Karpagam Academy of Higher Education Coiambathore

Dr. S Veni, department of Computer Science Karpagam Academy of Higher Education Coiambathore

Traditional public key solutions for nonrepudiation and authentication are computationally complex and are slow, not a benchmarked solution for a constrained environment [4]. With the evolution of Bring Your Own Devices (BYOD) concept, the IoT devices are unavoidable and emerging gadgets in business field. Implementations of cryptographic algorithms for IoT help to ensure security in the environment and the services trustworthy.

The common practice in an organization to restrict the access is to validate the users by a shared password. Normally an admin-selected password is shared by all users in the environment. If any user is vulnerable then it will affect the total security. Without proper hashing the scenario will compromise the entire environment.

When the algorithms are designed and implemented for IoT, two things need be kept in mind: 1) the algorithms should be cheap in case of resources and 2) it should be capable of offering medium level security. The existing light weight researches provide enough solutions for securing IoT [5][6][7][8]. This work tried to solve the issues related to BYOD to the environment and restrict access to a trusted server.

II. SYSTEM ARCHITECTURE AND COMPONENTS OF AUTHENTICATION SYSTEM

In IoT heterogeneous devices are able to remotely connect to the network on the fly necessitating the requirement of security. Monitoring an organization's security perimeter is crucial for intrusion detection to control unauthorized access [9]. Also, it is not practical for an administrator to scan each individual association request. For implementing security, a virtual environment is created to access the security of the proposed algorithm. For that a network with a Wi-Fi router and change in the default user ID and password of the Access Point needs to be set up.

A. Authentication Server

Authentication server is a high-end workstation connected to the network and authenticates all the devices before connecting to the servers. The authentication server creates a profile of the devices that are permitted in the environment and stored. For creating the profile, the server concatenates the Serial number, product ID and MAC address of the device. When a device is trying to connect with a protected server, Authentication server shares the curve parameter to the device. The pictorial representation of the process is given in figure1. Authentication server is also responsible to verify the signature received from the client device and it allows connectivity with the protected resource server as shown in figure2. Because of automatic connectivity of IoT devices, it is allowed to be part of the networked environment; so access restriction is a must to protect the trusted resources. [10]