© 2014 IJIRT | Volume 1 Issue 10 | ISSN: 2349-6002

Simulation of Protection from Illegal Attacks in M2M Communication Using DEAS

J.Sangeethapriya [1,]R.Dharengini [2], R.Priya[3], R.Sivaranjani[4], S.Vishnu Priya[5]
Saranathan college of Engineering, Trichy 620 002, TamilNadu, India

***Abstract*- Machine to Machine (M2M) communication is characterized by involving large number of intelligent machines sharing information and making collaborative decisions without direct human intervention. For many M2M communications secure authentication is more important than keeping confidentiality. In this system, dynamic encryption algorithm mechanism has been proposed to mutually authenticate users. A dynamic ID generation mechanism generates one-time-password (Either it may be number or text). The proposed dynamic-encryption scheme could avoid directly stealing and modifying of the IDs of the users. It has ability to withstand Phishing attack, online guessing attack, impersonation, brute force attack and insider attack. Our proposed system includes number of cryptographic algorithms such as Advanced Encryption Standard (AES), RIPEMD-160 (Race Integrity Primitive Evaluation Message Digest) and Random Generation Algorithm. The proposed system is simulating the ATM activities (service) with more security and authentication by the help of DEAS.**

***Index Terms*- Network security, Authentication, M2M, Attacks, Dynamic Encryption.**

I. INTRODUCTION

A specialized field in computer networking that involves securing a computer network infrastructure. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. Network security is typically handled by a network administrator or system administrator who implements the policy, network and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that users have adequate access to the network and resources to work.

Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. When developing a secure network, the following need to be considered

- Access – authorized users are provided the means to communicate to and from a particular network
- Confidentiality – Information in the network remains private
- Authentication – Ensure the users of the network are who they are
- Integrity – Ensure the message has not been modified in transit
- Non-repudiation – Ensure the user does not refuse that he used the network

A bandwidth efficient cooperative authentication (BECAN) scheme has been proposed to filter false reports in the M2M communication [3]. The scheme is designed to prevent the node compromising attacks which could not be detected because the compromising happens when the M2M nodes switch to a sleep mode. By the CNR-based mechanism, when a compromised M2M node sends false data to the gateway, the false data can be filtered if there is at least one uncompromised neighboring node participating in the reporting. However, the scheme has not addressed to protect the system from other types of attacks, such as denial of service (DoS) attacks, reply attacks, etc.

A novel approach for over-the-air automated authentication and verification of the M2M wireless sensor networks has been described using the existing authentication assets of a cellular telecom operator [4]. They extend the standard Generic Bootstrapping Architecture (GBA) provided in the 3GPP specifications to implement their solution. By the solution, the coordinator node authenticates itself to the cellular operator and derives key material. The shared key material is then used to securing the subsequent communication between the coordinating node and the M2M sever. However, the extension of the existing GBA may not be feasible.

Motivated to improve the security functionality of the M2M communication with much more robust authentication schemes, in this work, a dynamic-encryption authentication between mobile devices and the M2M service provider (MSP) and a mutual authentication between the mobile devices and sensor nodes with low cost have been designed and formally verified. Their contributions made in this paper can be

summarized up as follows [5]. (1) A dynamic encryption algorithm mechanism has been proposed to mutually authenticate mobile devices and the MSP. (2) A dynamic key generation mechanism which utilizes an initial key space and a seed to generate a one-time-password with low costs. Moreover, the level of security can be adjusted by changing the frequency of initial key materials updating. (3) A lightweight encryption algorithm has been employed to encrypt the messages transmitted among the mobile devices, sensor nodes and the MSP.

A simple architecture of the M2M service has been proposed to support an application in a hospital with the consideration of the mobility of doctors and patients [6]. An efficient security scheme with dynamic ID-Based authentication has been devised in the M2M system. The proposed scheme utilizes pair wise key pre-distribution to establish a key between the mobile sink and a sensor node. Then the mechanism uses a dynamic ID-Based authentication and collision-resistant hash function, to authenticate the source of the beacon signal before sensor nodes transmit their collected data to the mobile sink. The security analysis indicates that the proposed scheme could withstand the impersonation attacks due to the usage of the dynamic ID. However, the mechanism has a shortcoming to easily disclose the IDs of the sensors and the mobile device. And it cannot handle DoS attacks and reply attacks

The reminder of this paper is organized as follows. In Section II, the preliminary for our scheme is introduced. In Section III, the proposed scheme is presented in details. The security analysis of our scheme is presented in Section IV .Finally, the paper is concluded in Section V.

II. PRELIMINARY

A.M2M System Model

The M2M system model used in our scheme shown as Fig.1. It consists of user, browser, Login credentials, security engine, and database.

User: She/he is entering into the application through the web browser to register and login into their account.

Browser: A Web browser is a client program that uses HTTP (Hypertext Transfer Protocol) to make requests of Web servers throughout the Internet on behalf of the browser user.

Login credentials: It includes the registration process by giving the user details such as account number, initial deposit and also includes personal details. User has to select the random image given by the server and also she/he has to give the security question with answer during registration. A login credentials also consists of logging into their account by giving the user name and password. Before proceeding into their account, she/he has to select the random image which is already selected during the registration process.

Security Engine: It comprises of all the Security Protocols and algorithms such as AES, Triple DES, MD5, salt algorithm, and RIPEMD. Security Engine exists both in the user's end as well as Server's end.

Database: Database contains the user details which are entered in the login credentials.

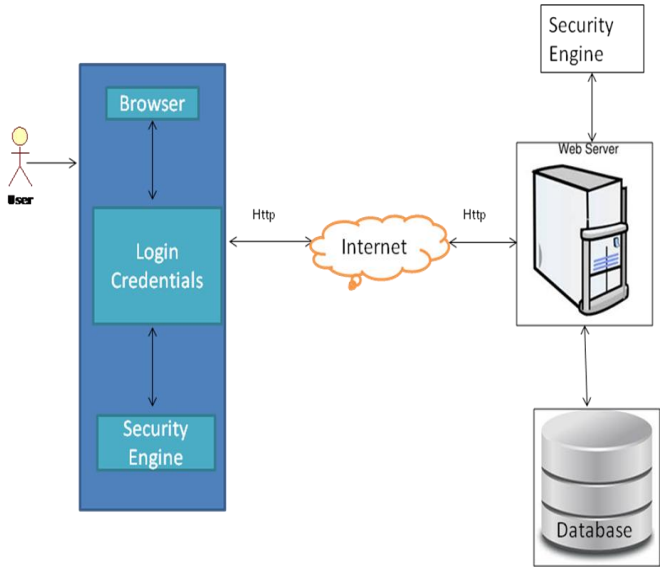

Fig. 1

B. Abbreviations and Acronyms

The abbreviations and acronyms used in our proposed scheme are: M2M communication, DEAS, AES, Triple DES, Hash MD5, IBS, RIPEMD and OTP.

M2M - Machine to Machine Communication.
DEAS - Dynamic Encryption Authentication Scheme.
AES - Advanced Encryption Standard
Triple DES - Triple Data Encryption Standard
Hash MD5 - Hash Message Digest 5
IBS - Identity Based Signature
RIPEMD - Race Integrity Primitive Evaluation Message Digest.
OTP - One Time Password

III. DETAILED PRESENTATION

Our project consists of three modules such as Login process, Dynamic Encryption and Random ID generation.

This scheme composed of many algorithms such as AES, Triple DES, MD5, and RIPEMD. OTP is generated with the help of Random generation algorithm, which selects the number dynamically.

Login process: The user has to register their details such as username, password, account number, initial deposit, etc. by entering in the website. The user must enter the security questions and image for the security purpose. By using security encryption algorithms entered details are encrypted and stored in the Database. Then the user has to login with their username and password with many levels of security. Database authenticates the user after which the user undergoes the further processing.

Dynamic encryption: This module includes the process of withdrawal. If the user wants to withdraw the amount, they have to verify their account using digital authentication, which was initially created by Database. The digital authentication is created and stored with the help of Identity Based Signature (IBS) mechanism. After, Web server generates One Time Password (either text or number). That OTP is generated with the help of Random generation algorithm.

Random ID generation: This module includes the processes such as Mini statement display, Balance enquiry, Password settings.

Mini Statement: In case if user wants to view the recent transactions, he/she has to request the Server for the mini statement. Server will send the one time password to the user. Then the browser will display the mini statement.

Balance enquiry: If user is requesting for their balance enquiry, Database will display the details of the balance.

Password settings: If the users want to change their password, they will request the Server for one time password (as text or number). After changing the password, Database is updated with the new password.

IV. SECURITY ANALYSIS

In this section, we will analyze the security function of our authentication scheme.

Mutual Authentication: Mutual authentication is a security feature in which a client must prove its identity to a server and server must prove its identity to client. It also refers as two way authentication, in which two parties authenticating each other at same time. In this way, the users can be assured that they are registering/logging into legitimate entities and servers can be certain that all would be-users are attempting to gain access for legitimate purposes. Mutual authentication is gaining acceptance as a tool that can minimize the risk of online fraud at ATM banking services. In our proposed scheme, Mutual authentication is achieved with the help of sending One Time Password (OTP) to the user's registered mail ID. OTP is generated by Random Generation Algorithm. Random number is generated and is encrypted by using algorithms such as Hash MD5, Triple DES, and AES.

After received the OTP, the user has to verify and validate, and they will be allowed to further processing activities such as Withdrawal, Mini Statement, Balance enquiry and Change Password.

Ability against Phishing Attack: Phishing is e-mail fraud method in which the perpetrator sends legitimate looking e-mail in an attempt to gather personal and financial information from users. It is a form of online identity theft in which fraudsters trick Internet users into submitting personal information to illegitimate websites. Phishing email will direct the user to visit a website where they are asked to update personal information, such as password, credit card number, bank account number, etc. that the legitimate website already has. The website, is however bogus and set up only to steal the information of the users that enter on the page. In our proposed project, Phishing attack can be overcome by using RIPEMD algorithm.

Ability against Man-in-the-middle Attack: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. It is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. In our paper, for every transaction (activity), OTP will be send to the user for authentication purpose. Thus the Man-in-the-middle attack can be prevented.

Ability against Impersonation Attack: Impersonation is the ability of a thread to execute in a security context that is different from the context of the process that owns the thread. Impersonation is designed to meet the security requirements of client/server applications. When running in a client's security context, a service "is" the client, to some degree. One of the service's threads uses an access token representing the client's credentials to obtain access to the objects to which the client has access. The primary reason for impersonation is to cause

access checks to be performed against the client's identity. Using the client's identity for access checks can cause access to be either restricted or expanded, depending on what the client has permission to do. In our proposed scheme, mail will be send to the authenticated users, only they can open the mail and will receive the password. This implies that it is impossible for a third person to act as a legitimate user. Thus the Impersonation attack can be avoided.

Ability against Brute force Attack: A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack may also be referred to as brute force cracking. In our proposed scheme, brute force attack can be prevented by giving a few trials to the user while selecting the random image and security questions (which is selected during registration process)

Ability against Online guessing Attack: Another type of network attack is Password Guessing attack i.e. online guessing attack. Here a legitimate users access rights to a computer and network resources are compromised by identifying the user id/password combination of the legitimate user.

V. CONCLUSION

In order to protect the user's privacy and property from illegal attacks in M2M communication, in our paper, a dynamic-encryption authentication scheme has been designed and formally verified. This scheme can ensure a safe session between machine communications. This proposed dynamic-encryption scheme could avoid directly stealing and modifying of the IDs of the users who are having accounts. The dynamic ID generation mechanism provides a reliable one-time-password to the users. Our project shows that the mutual authentication and the ability of withstanding multiple attacks could be prevented.

Future analysis can be done, with the help of our proposed scheme, if it will be implemented in ATM.

REFERENCES

[1] Ami Damian, Wooyoung Soh, Seoksoo Kim "Adaptive Identity-Based Signcryption for Dynamic Source Routing in Machine to Machine Networks"

[2] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, Mike Meyerstein "Security and Trust for M2M Communications"

[3] Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen, University of Waterloo "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications"

[4] Sachin Agarwal, Christoph Peylo, Ravishankar Borgaonkar, Jean-Pierre Seifert"Operator-based Over-the-air M2M Wireless Sensor Network Security"

[5] Shuo Chen and Maode Ma "A Dynamic-Encryption Authentication Scheme for M2M Security in Cyber-Physical Systems"

[6] Tien-Dung Nguyen and Eui-Nam hah, Department of computer Science,Kyung Hee University,Korea "A Dynamic ID based authentication scheme for M2M communication of Healthcare Systems"