Cryptanalysis and Improvement of Barman et al.'s Secure Remote User Authentication Scheme

Chintan Patel, Nishant Doshi

***Abstract*—** In past people used to send the messages in plain text over the public channel. However, this protocol susceptible to various attacks like anyone can read the message, no proper authentication of sender and receiver, tampering, etc. Indeed, Remote User Authentication (RUA) is a technique is the key to solution of all these problems. RUA is scheme in which any remote user can not only authenticate but also transfer the messages over insecure medium to server even though the extraneous physical distance between them. With advancement in technology, the system moved to multi server in which user can connect to the any server and have the secure established session over public channel. Recently, in IEEE Access, Barman et al. proposed the multi-server remote user authentication scheme using the notion of fuzzy commitment and claimed to secure against various attack. However, in this paper we prove that the scheme due to Barman et al. is failed to provide the countermeasure against *user anonymity, server anonymity, Stolen Verifier Attack and perfect forward secrecy attack, lack of level-based authentication*. In this paper, we also propose the novel level dependent authentication scheme for the environment where user wants to get access of live data from the sensor via gateway device. At last, we provide informal security analysis for the proposed scheme. We conclude this paper with some future direction.

***Keywords*—**Multi-Server, Fuzzy Commitment, Information Security, Level-based authentication.

I. Introduction

In today's world, Information and Communication Technology (ICT) is the key point for any nation to progress. Indeed, ICT relies on the advancement of the technology and importantly the communication. In data communication, not only the speed matters but also security plays vital role due to nature of data. One way to achieve this is to establish the secure communication between all participating entities. However, it will be costly in installation as well as maintenance. In 1981, Lamport [1] proposed the first remote user authentication technique in which any remote user can establish the secure session over the public channel and also authenticate each other too.

Chintan Patel is PhD Scholar with the Computer Science and Engineering Department, Pandit Deendayal Petroleum University, Gandhinagar, India (e-mail: Chintan.p592@gmail.com).

Nishant Doshi is faculty with the Computer Science and Engineering Department, Pandit Deendayal Petroleum University, Gandhinagar, India (Contact : 792-327-5458 e-mail: doshinikki2004@gmail.com).

These communication systems broadly classified in two categories i.e. single server and multi-server. In single server, only single point of server is there to which all users will connect. In multi-server, more than one server is available, and users are required to connect to either server for possible communication. in general, one Resource Center (RC) will be there for initial setup. Each of the single and multi-server system is categorized either into two factors or three factor schemes. In two factors only the identity and password with smart card is considered while in three factors scheme the biometric identity of user also considered in addition to identity and password.

In [2-22], the authors have proposed the single server-based schemes. In [23-38], the authors have proposed the multi-server-based schemes. Recently in 2018, Barman et al. [39] proposed the multi-server scheme based on the fuzzy commitment analysis and claimed that it is secure against various attacks.

A. Our Contributions

In this paper we have cryptanalysis the fuzzy based multi-server three factor authentication scheme which proposed by the Barman et al. We have shown the following attacks in the scheme of barman et al.

- User anonymity
- Server anonymity
- Perfect Forward secrecy
    - By compromising user's secret credentials
    - By compromising server's secret credentials
    - By compromising RC's secret credentials
- Stolen Verifier Attack

In this paper, we also propose novel ECC based level dependent authentication scheme which is also suitable for Wireless Sensor Network (WSN) and IoT based environment. By keeping the real time scenario in the mind, as an improvement of the proposed scheme, we propose the authentication scheme for User -Gateway/Server – Sensor based environments.

B. Paper organization

In Section II, we have given the preliminaries that we will use throughout this paper. In section III, we have given the