International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

RESEARCH ARTICLE

ISSN: 2321-7758

A SECURE USER MUTUAL AUTHENTICATION OF SENSED DATA AND STORING IT IN CLOUD

TENZIN DHEKYONG[1], GEETHA.S[2]
[1]M.tech, CSE, CMRIT, Bangalore,India
[2]Associate Professor, Department of ISE, CMRIT, Bangalore, India

ABSTRACT
Sensor network is an important approach of data capturing. User authentication is a critical security issue for sensor networks because sensor nodes are deployed in an open and unattended environment, leaving them possible hostile attack.In this paper, we show that the mutual authentication can be done with security while sending data from user to gateway with help of sensors. Once the mutual authentication is completed, then the data is stored in cloud for security and for using the data in future.

Keywords—Wireless Sensor Networks, Mutual Authentication, Sensors, Gateway.

INTRODUCTION

Wireless sensor networks are spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Wireless Sensor networks (WSNs) is an open environment distributed network, which is an important approach of data capturing for big data. Nevertheless, with the application of Big data, the requirement of real-time data from WSNs is increasing highly. In some situations the gateway impossibly does force a user to access the sensor node directly. In such case the security and reliability to inquire and data disseminate are very important. Only when every client in the WSNs proves his/her identity can he/she be allowed to join the WSNs and access to resource, such as real time data. Thus, a key security requirement for WSNs is user authentication.

Overview and related works

Existing System

The Existing System has following shortcoming :

- No full mutual authentication .
- No key agreement between the user and the sensor node.
- No prefer forward security.
- No protecting against insider attack,forgery attack and DoS attack.
- Sensor node revealing and exposing the password to the other node and
- No updating user's password.

Proposed System

The Advantages are as follows:

The proposed protocol provides message confidentiality service.

The proposed protocol resists:

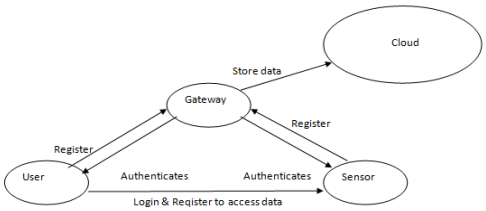
- An integrity attack,
- Denial attack,
- DoS Attack,
- Sensor node compromise attack,
- Replay attack,
- An impersonation attack,
- A stolen verifier attack,
- An insider attack, and
- A man-in-the-middle attack.

Disadvantage:

- No full authentication between Sensor and User.

System Design

The process of defining the architecture, components, modules, interfaces and data for a system to satisfy specified requirements.



The system architecture describes about the working of the system.The user registers with the gateway and gets authenticated from it.The user login and register to access data from the sensor and then gateway informs if the user is authenticated or not to the sensor.Gateway stores the sensed data to the cloud for the security and for the future usage.

This system which included three phases:

Setup phase, Login phase and Registration phase and Password update phase.

Setup Phase

when setting up the base station or gateway,it generates randomly the public key and private key which are prime numbers.

Login Phase and Registration Phase

The user will first need to register and then login ,after which a dialog box pops up and we need to mention the type of node of sensor to be used.

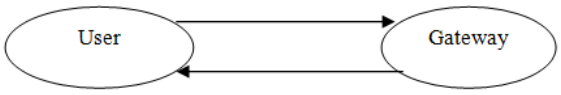
Password Update Phase

The previous password can be updated in case if we forget the previous password which has been used.

Future Enhancement

Mutual Authentication Phase is the enhanced work in this paper.In this phase,we use Diffie-Helman algorithm.

Diffie-Helman algorithm is explained as follows:



1.User and Gateway agree on a prime number p and a base g.

2 User chooses a secret number a, and sends Gateway (g a mod p).

3 Gateway chooses a secret number b, and sends User (g b mod p).

4 User computes ((g b mod p) a mod p).

5 Gateway computes ((g a mod p) b mod p).

User and Gateway share the same g value.

Using Diffie Helman algorithm, Share key is generated for both user and gateway .

If they have same shared key then it shows that they are mutually authenticated.

If they do not have the same shared key then they are not mutually authenticated.

b)Storage of Sensed data in Cloud

As we need paid account for using real cloud so,we are using dropbox as the cloud to store the sensed data for the security and for future reference.

The gateway stores the sensed data in the cloud i.e dropbox.

Conclusion

In this paper, we discussed about the secure user of mutual authentication of sensed data and how it is stored in cloud.We have analysed the proposed system using the references and we extended the future enhancements. The proposed protocol, which does not provide mutual authentication between user and sensor node and confidentiality service, is susceptible to insider, replay, denial, compromise, forgery, man-in-the-middle and DoS attacks.We have also reviewed the existing protocols ,which does not provide mutual authentication and protect against insider, denial, compromise, man-in-themiddle and DoS attacks, of Das, which is vulnerable to forgery, denial, compromise, DoS, man-in-the-middle attacks.Since WSNs need more secure mutual authentication method in an insecure network environment, we use the IBE mechanism to design a new user authentication protocol.

For future enhancement,Protocol provides Mutual authentication between user and sensor node,Protocol makes use of cloud for storing data.

References

[1]. Zhou Quan, Tang Chunming, Zhen Xianghan,and Rong Chunming “A secure user authentication protocol for sensor network in data capturing.”Quan et al. Journal of Cloud Computing: Advances, Systems and Applications (2015)

[2]. Das ML, Saxena A, Gulati VP (2004) A dynamic ID-based remote user authentication scheme. IEEE Trans Consum Electron 50(2):629–31

[3]. Leung KC, Cheng LM, Fong AS, Chan CK (2003) Cryptanalysis of a modified remote user authentication scheme using smart cards. IEEE Trans Consum Electron 49(4):1243–5.

[4]. Tseng HR, Jan RH, Yang W (2007) An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM'07), 986–990.

[5]. Ko KC (2008) A novel dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Symposium on Wireless Communication Systems, ISWCS'08, 608–612.

[6]. Yeh HL, Chen TH, Liu PC, Kim TH, Wei HW (2011) A secured authentication protocol for wireless sensor networks using elliptic curves cryptography.Sensors 11(5):4767–79.