International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 9 (September'2017)

AN EFFICIENT BIOMETRIC BASED USER AUTHENTICATION SCHEME IN WSN USING ARTIFICIAL BEE COLONY ALGORITHM

D.Thamaraiselvi,
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
Kanchipuram,Tamilnadu,India.

Dr.M.Ramakrishnan,
Professor,
Department of Information Technology,
Madurai Kamarajar University,
Madurai,Tamilnadu,India.

Abstract: User authentication is a crucial service in wireless sensor networks (WSNs) that is becoming *increasingly common in WSNs because wireless sensor nodes are typically deployed in an* unattended environment, leaving them open to possible hostile network attack. The main goal of the paper is to securely authenticate remote user in a convenient and user friendly manner. In this paper, we propose a Biometric (finger print) based user authentication scheme using ABC algorithm in hierarchical wireless sensor networks. The proposed scheme includes three phases for user authentication such as registration phase, login phase and authentication phase.

Keywords: Finger print, ABC, Authentication, WSN.

I. INTRODUCTION

Remote user authentication is a method to authenticate remote users to a server over insecure networks . In today's electronic era, smart card based remote user authentication schemes are widely acknowledged as one of the most secure and reliable forms of electronic identification .Wireless sensor networks (WSNs) are applied widely a variety of areas such as military, environmental monitoring, real- time traffic monitoring, measurement of seismic activity, wildlife monitoring, medical, building condition monitoring and so on. Remote User authentication in WSNs is a critical security issue due to their unattended and hostile deployment in the field to deal with secret data over insecure networks. With the help of remote user authentication schemes, people can interact with the server through distributed or portable terminals. In a remote user authentication scheme, the authenticity and integrity of the user and the server are important elements over an insecure network. At their best, the remote user and remote server can securely authenticate each other, processing and protecting the communication in a convenient and user friendly manner.

Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used.

There are no proper ad hoc infrastructures in wireless sensor networks where a large number of sensor nodes are deployed by truck or plane on a target field. After deployment of sensor nodes, they communicate to other neighboring nodes within their communication range to form clusters. After that, one cluster head or gateway node is selected by base station or sensor nodes for each cluster on the basis of energy, signal strength, degree, capability, mobility etc. All the sensor nodes sense raw data from environment and send to their nearest cluster head by single-hop or multi-hop communication .Cluster heads gather the raw data and send to nearest base station or sink node by multi-hop or single-hop communication .Finally, data are collected from base station. The collected data is not always real time data because all cluster heads send data to base station after a certain periodic time. If we collect data directly from cluster heads, we can get real time data. This is possible if it is allowed to access those real time data directly from cluster head, when demanded. Hence, it is needed to first authorize the accesses and then allows to access to do secure communication among accesses and cluster heads .

II. RELATED WORK

Jianjun Yuan,Changjun JiangZuowen Jiang[1]Proposed biometric based user authentication protocol in wsn. In that protocol they used biometric keys,that scheme cannot resist threats. It uses hash function by which it has more computation time and communication cost .In 2016 Youngung choi,youngsook lee and Dongho won[2] proposed biometric based user authentication scheme using fuzzy extraction. This scheme uses fuzzy ,fuzzy could not provide exact authentication and it has security threats. In 2015 Das, Ashok Kumar ble Chaterjee , Santanu , Sing Jamuna Kanta[3] proposed new biometric based remote user authentication scheme in hierarchical wireless body area sensor networks which uses both biometric and password for verification and allows the users to access real time data . this scheme has the draw back of password stolen attack.Yoon, Eun-Jun; Kim, Cheonshik[4] proposed Advanced Biometric-Based User Authentication Scheme for Wireless Sensor Networks which uses one way hash function . this scheme uses hash function ,so it more computational time and communication cost for user authentication in wireless sensor networks Tanmoy Maitra, Ruhul Amin, Debasis Giri and P. D. Srivastava[5] proposed smart card based user authentication user authentication , smart card is used by the user for accessing the data , this scheme coludn't with stand in smart card breach attack.In 2015 Ashok kumar das [6] Proposed biometric based user authentication scheme using smart card and fuzzy extractor and this scheme has the draw back of smart card breach attack.

III.PROPOSED ABC METHOD

The proposed scheme uses finger print to authenticate the user who is accessing the data in a hierarical wireless sensor network. In this scheme ABC algorithm is used for matching of the finger print for authentication purpose , this scheme has three phases a.Registration phase b. Loginphase c.Verification phase.

ABC ALGORITHM FOR MATCHING:

The Artificial Bee Colony Algorithm is a swarm based optimization algorithm proposed for the first time by Karaboga in 2005. There are three kinds of honey bees in ABC algorithm to forage food source. They are employed bees, onlookers and scouts bees. The tasks of these bees are to collect nectar around the hive. A bee waiting on the dance area for making decision to choose a food source is called an onlooker and a bee going to the food source previously visited by it is named as an employed bee. A bee carrying out random search is called a scout bee. In ABC, food searching and nectar foraging around the hive are performed by employed, onlooker and scouts bees collectively. In the ABC algorithm, the first half of the colony consists of employed artificial bees and the second half constitutes the onlookers. For every food source, there is only one employed bee. In other words, the number of employed bees is equal the number of food sources around the hive. The employed bee whose food source is exhausted by the employed and onlooker bees becomes a scout.

The ABC algorithm is used for calculating the biometric minutiae of finger print for user authentication . Biometric is an unique feature for human identification .Biometric minutiae can calculated by the following process

Step 1: Binarization

Binarization is the process of converting a grey scale image into binary image. Global threshold value is used .

Step 2: *Thinning*

The objective of thinning is to find the ridges of one pixel width. The process consist in performing successive erosions until a set of connected lines of unit-width is reached. An important property of thinning is the preservation of the connectivity and topology which however can lead to generation of small bifurcation artifacts and consequently to detection of false minutiae.

Step 3: Minutiae detection

From the binary thinned image, the minutiae are detected by using nxn pattern masks. Samples of masks used for identifying the ridge ending and bifurcations point. After a successful extraction of minutiae, they are stored in a template, which may contain the minutia position (x,y), and minutia type (bifurcation or termination). After detecting the points, the standard deviation SD of the minutiae points can be calculated as,

$$SD = \sqrt{\frac{1}{N\sum_{i=1}^{N}(m_i - \mu)}} \quad \rightarrow (1)$$

In which, the mean value $\mu = \frac{\sum_{i=1}^{N} m_i}{N}$ for $i = 1, 2, \cdots, N$ and m_i is the extracted minutiae points.

In the same way the minutiae are detected for the query image and these also stored as template. During the enrolment, the stored standard deviation values will be used in the matching process as reference template or database template. During the verification or identification, the extracted minutia are also stored in a template and are used as query template during the matching.

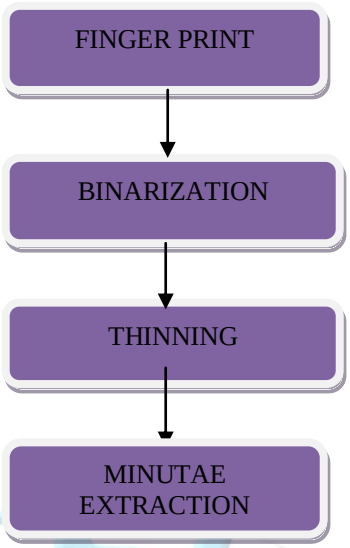

Figure 1:Biometric minutiae feature extraction

Authentication scheme

The Authentication scheme has three phases

- login phase
- registration phase
- verification phase

A.Registration phase :

In the registration phase the user can register by giving username and password and his or finger print from the finger print of the user the standard deviation is calculated and stored .

B.login phase

In the login phase the user can login by using username ,password and finger print

C.Verification phase

In the verification phase the standard deviation of finger print is matched with the stored SD value using ABC algorithm . if there is match then the user is legitimate user to access the wsn data . if the is no match then user is not a legitimate user.

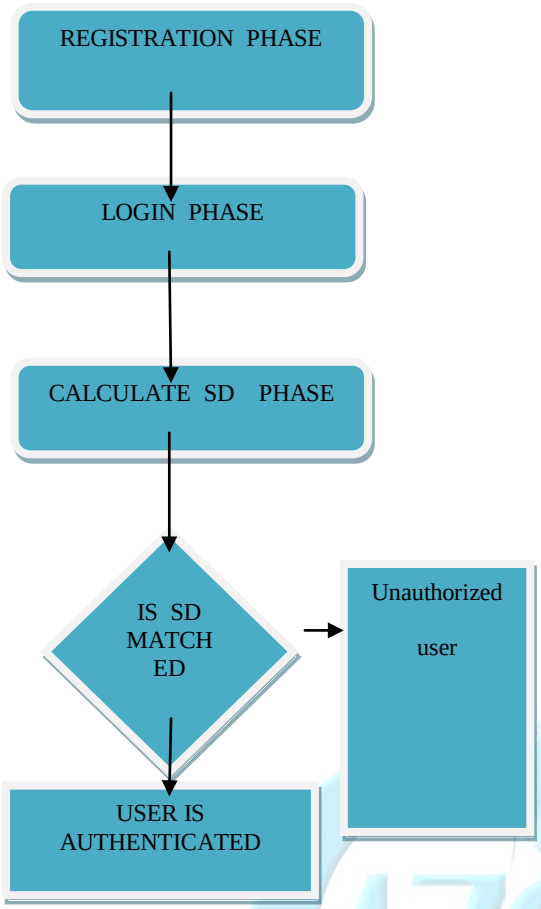

Figure2:Authentication Process

IV.CONCLUSION

In this paper user is authenticated using biometric finger print data where the features are extracted and stored in base station when a user wants to access the data he has to insert smart card and the finger .The standard deviation is calculated using artificial bee colony algorithim for searching in an optimized way.

V.REFERENCES

[1] Awasthi A. K. and Lal S, "A remoteuserauthentication scheme using smarts cards with forward secrecy," IEEE Trans. Consumer Electronic, vol. 49, no. 4, pp. 1246-1248, 2003.

[2] Chan C. K. and Cheng L. M, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consumer Electronic, 46, pp. 992-993, 2000.

[3] Leung K. C., Cheng L. M., Fong A. S. and Chen C. K, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consumer Electronic, 49-3, pp.1243-1245, 2003.

[4] Lee S. W., Kim H. S. and Yoo K. Y, "Comment on a remote user authentication scheme using smart cards with forward secrecy," IEEE Trans. Consumer Electronic, 50, 2: pp. 576-577, 2004.

[5] Liaw H.T., Lin J.F. and Wu W.C., "An efficient and complete remote user authentication scheme using smart cards," Mathematical and Computer Modelling, 44, pp. 223-228, 2006.

[6] Shen Z. H, "A new modified remote user authentication scheme using smart cards," Applied Mathematics, Volume 23-3, 371-376, 2008.

[7] M. T. Thai, F. Wang, D. Liu, S. Zhu, and D. Z. Du, "Connected dominating sets in wireless networks with different transmission ranges," IEEE Transactions on Mobile Computing, vol. 6, no. 7, pp. 721– 730, 2007.

[8] F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," International Journal of Network Security, vol. 7, no. 1, pp. 61–68, 2008.

[9] R. Fan, L. di Ping, J. Q. Fu, and X. Z. Pan, "A secure and efficient user authentication protocol for two tiered wireless sensor networks," in Second Pacific Asia Conference on Circuits, Communications and System (PACCS'10), vol. 1, pp. 425–428, 2010.

[10] D. He, Yi Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," Ad Hoc & Sensor Wireless Networks, vol. 10, no. 4, pp. 361–371, 2010.