International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

A RELIABLE USER AUTHENTICATION SCHEME FOR HEALTHCARE MONITORING IN WIRELESS SENSOR NETWORKS

Dr. G.Santhi
Assistant Professor Dept. of Information Technology Pondicherry Engineering College, Puducherry
shanthikarthikeyan@pec.edu
R. Sowmiya
Student of M.Tech (IT)
Dept. of Information Technology
Pondicherry Engineering College, Puducherry
sowmidas25@pec.edu

***Abstract*—** For past few years, more interest has been focused on Wireless Sensor Networks (WSN) due to its wide range of applications in various fields. The WSNs are mainly used for sensing the pollution, monitoring the traffic; secure homeland, hospitals, military etc. These sensor networks face many challenges due to the use of wireless medium for communication which is prone to various types of attacks resulting in loss of information. The security requirements in WSN include four major aspects; data confidentiality, data integrity, data authentication and data freshness. Cryptography is used to cater these requirements. Here, a secure cryptosystem was applied using both Bilinear Pairing and Digital signature for establishing a secure user authentication. This paper proposes an efficient user authentication scheme that facilitates security and privacy protection; enable medical personnel to continuously monitor the health conditions of patients and provide a sophisticated medical care.

Keywords: WSN, Bilinear Pairing, Digital Signature.

I. INTRODUCTION

Wireless Sensor Networks (WSN) is composed of hundreds of thousands of tiny devices called nodes [1]. A sensor node is often abbreviated as a node. The basic units of WSN are nodes (sometimes called motes). A Node consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transmitter for forming an ad hoc network. A Node and Sensor together form a Sensor Node. There can be different Sensors for different purposes mounted on a Node.

The general purpose of WSN is to monitor some physical phenomena (e.g., temperature, barometric pressure, light) inside the area of deployment. Due to the size and expected costs of the nodes, they are constrained in processing power and energy. The number of nodes deployed in WSN can vary from tens to tens of thousands depending on the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

particular application. Nodes can be deployed, for example, by precise placing one by one into predefined positions or by dropping from the plane. Their positions can be static or mobile. Networks with nodes in static positions are more common. Nodes have to be autonomous and the network itself has to be self-organizing.

Security in sensor networks is a very important factor. It is important to make sure that the sensitive information are well protected to maintain the confidentiality and avoid revealing the data to an unauthorized third parties, otherwise it may result in eavesdropping on the communication. The identity of the participants in a communication should be verified by an authentication technique to ensure the data received was sent by a trusted sender. Lack of integrity may result in inaccurate information. The message reply attack is one of the many attacks launched against sensor networks where an adversary may capture messages exchanged between nodes and reply them later to cause confusion to the network.

II. LITERATURE SURVEY

A. Continuous Leakage-Resilient Certificate-Based Encryption (CLR-CBE)

The Certificate-Based Encryption (CBE) was first proposed by Gentry [2]. The main idea is to adopt secret sharing to split a private key. The private key is divided into two secret states. One of the secret states is updated in the first stage of decryption and calculates a value. The other secret state is updated in the second part of decryption and computes the plaintext. This scheme is secure against continuous leakage attacks and adaptive chosen ciphertext attacks. The disadvantage of using this scheme is the adversary has the capability to obtain a certificate of each user and the adversary can learn at most N bits for leaked secret data per invocation for the cryptographic primitive, but is banned to replace any users public keys. There is a possibility of leakage of master key and random value.

B. Merkle Hash Tree Based Authentication Scheme

Merkle trees were first described by Merkle in 1979 [3]. The Merkle tree is a complete binary tree where the internal nodes are one-way functions of the values of their children. The main idea of Merkle hash tree is to construct a tree based on a one-way cryptographic hash function h(.). The biggest problem of one time signature schemes is key management. The public key must be guaranteed to be belonging to the intended communication partner. If the nodes of the tree are not stored, the nodes must be generated again for every signature. Generating the tree is very expensive, so that generating the entire tree for every signature is impracticable for bigger trees. But saving all $2n+1-1$ nodes could result in large storage requirements. Hence, a good strategy is needed, to generate the signature without saving too many nodes, at a still efficient time.

C. Digital signature based Authentication Scheme

Digital signature of a message is a number which is known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable to check whether the user is legitimate or not. The third party should be able to resolve the matter equitably, without necessitating access to the signer's private key. The first method

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

discovered was the RSA signature scheme, and the other is Feige-Fiat-Shamir signature scheme requires a one way hash function.

III. SYSTEM ARCHITECTURE OF RELIABLE AUTHENTICATION MECHANISM

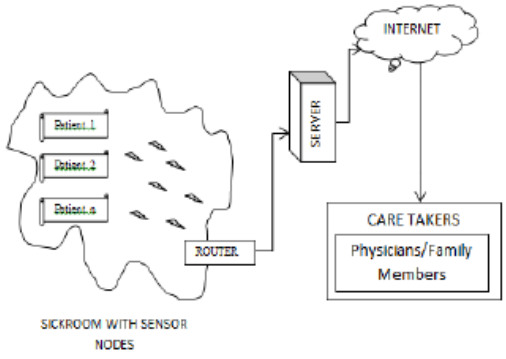
To enable security and privacy protection in the medical care system, this paper established the reliable and secure authentication system based on WSN. The professional caregivers verify the health conditions of patients at all times and provide with appropriate healthcare. This system protects the confidentiality and security of the user to prevent the intrusion and eavesdropping during data transmission. In this study, the targeted users of home tele-care systems were patients in hospitals and healthcare institutions or older people who necessitate medical care as shown in Fig.1. The system stores their physiological data continuously and then transmitted to the care centers. To capture the physiological data of the patients, the patients should wear the mobile care devices. The base station conveys the request to the sensor on patients, after receiving the request message the physiological data is transmitted to the base station. The transmission of data is done to the wireless routers fit in the healthcare institution or hospitals through wireless sensors. Later, the data are uploaded to the servers in care centers. When physicians or the family members wish to inquire information of patients, they must register with the Trust Authority (TA). After successful registration, the Trust Authority provides users with encrypted unique password. Users can then use the password to log into the tele-care system. The users can inquire and use the data of patients in hospitals or healthcare institutions installed with sensor nodes within a limited time, thereby legally acquiring the physiological data and medical information on patients.

A. End User Authentication Using Bilinear Pairing

End user authentication is the important one to check whether they are the correct end users. Here, the sender is nurse who continuously verifies the sensors and updates the information. The receiver is the care takers such as Physicians/Family members. The physician verifies the conditions of the patient and takes care of them by providing treatment. Family members can only review the condition. For the end user authentication, bilinear pairing is chosen.

1) Bilinear Pairing

The major pairing-based concept is the bilinear map. The two groups G1 and G2 of prime order q [5]. For clarity, it is denoted G1 using additive representation and G2 using multiplicative representation, although the group operations in G1 and G2 may well be very dissimilar from the well-known arithmetic addition and multiplication



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

Fig.1 System Architecture

Consider P and Q two generators of G1, and write a times

aP = P + P + . . . + P

Now consider the mapping e as follows: e: G1 × G1 → G2

Bilinear Mapping on (G1, G2) is: e: G1 × G1 → G2 that satisfies the following conditions:

1. Bilinearity: ∀ P Q ∈ G1 and a, b ∈ z ∗ p, e (aP, bQ) = e (P, Q)ab .
2. Non-degeneracy: e (P, P) is a generator in G2.
3. Computable: e can be easily computable.

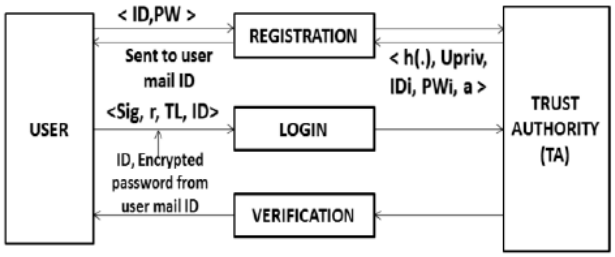


Fig.2 End User Authentication Using Bilinear Pairing

By using Bilinear Pairing algorithm, user Ui registers an authentication IDi with the Trusted Authority (TA) and sets a password PWi as shown in Fig.2. The TA includes the parameters <h(.),Upriv,IDi,PWi,a > where h represents a one-way hash function, Upriv represents the user private key, IDi represents the user id, PWi represents the password and a represents a private parameter generated by the TA and send it to the user. The user transmit <Sig, r, TL, ID>, where Sig represents Signature, r = h (ID || PW || a), TL represents the login time, to the TA and in verification phase it verifies whether the user is valid or not.

2) User Authentication

The first and most critical data protection measure is authentication [6]. User authentication involves identifying whether users are authorized users of a system, preventing illegitimate users from intruding the system for critical information. The most frequently used and convenient authentication mechanism in networks is password authentication, which necessitates users to be authenticated using their account names and passwords. When operators enter their account numbers and passwords to log into a system, the system verifies whether the given data are correct. When the data are verified to be accurate, the users are identified as legitimate users of the system; otherwise, the login requests of the users are denied. Even though using passwords for authentication is easy, if the passwords of users are too simple, there is a risk. To overcome this flaw, in the proposed work, the secret key from the mail ID of the user and password authentication systems are typically combined to complement the flaws of each other. The user authentication system is separated into three phases namely the registration phase, login phase, and authentication phase.

a) Registration Phase

Before user use a system, they must apply for the approval from an administrator. For registration, the user must send the data to the Trust Authority (TA) such as username, password and email id, only then the users are authorized to access the information in the system. Verify if user exists After registration, the Trust Authority (TA)

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

generates the secret key and send it to the user mail id.

b) Login phase

When user log into the system, they must enter the secret key provided by the administrator for an authentication and the secret key is only valid for 10 minutes. If the user login the user name, password and secret key, it checks the user is valid or not.

c) Authentication phase

The administrator then verifies whether the users are legal user by examining the user data such as user name, password and secret key, if the users are legal users then they would be allowed to access the information in the system and the unique key is valid only for certain time period, then the key is expired. Therefore, the new key is to be generated and it should be pasted.

B. Source Authentication Using Digital Signature

Source authentication is to be done, to verify whether the message comes from the correct source without any modification of physiological data (pulse rate, blood pressure, temperature etc.). In this paper, the source is represented as the nurse. The Digital Signature is used for the source authentication.

1) Digital Signature

The public-key primitives of message authentication are Digital Signatures [7]. In the corporal world, it is common to use handwritten signatures or typed messages. They are used to combine signatory to the message. Similarly, a digital signature is a method that binds a person/entity to the digital data. This binding can be individually verified by receiver as well as any third party. Digital signature is a cryptographic value which is calculated from the data and a secret key is known only by the signer.

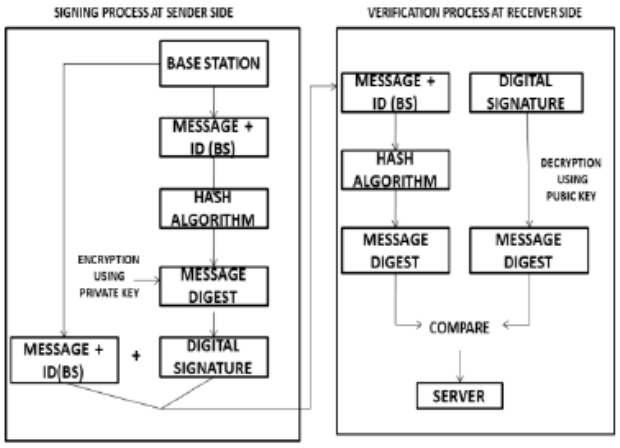


Fig.3 Source Authentication using Digital Signature

Each person has a public key and private key. Generally, the key pairs are used for encryption/decryption. The key is referred to as the signature key, if the private key used for signing process and the key is referred to as the verification key if the public key used for the verification process. To generate hash of data, signer feeds data to the hash function as shown in Fig.3. To produce the digital signature on given hash, hash value and signature key are then fed to the signature algorithm. Signature is added along with the data and then sent to the verifier. Verifier feeds the digital signature and the verification key (i.e) public key into the verification algorithm. The verification algorithm gives some numbers as output.

To generate hash value, verifier also runs the same hash function on received data. For verification process, this hash value and output of verification

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

algorithm are compared. Based on the comparison result produced, verifier decides whether the digital signature is valid or not. Since, digital signature is created by 'private' key of the signer and no one can have this key; the signer cannot reject signing the data in future. Notice as to be done that, a hash of data is to be created instead of signing data directly by signing algorithm. Since the hash value of data is a unique representation of data, it is necessary to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is effectiveness.

2) Digital Signature Mechanism

The digital signature algorithms generally consist of three sub phases, Key generation Asymmetric algorithm, signing algorithm and Signature verification algorithm.

The digital signature resists the following attacks such as

- Key-only attack: Adversary knows only the verification function (i.e) public key.
- Known message attack: Adversary knows a list of messages earlier signed by Alice.
- Chosen message attack: Adversary can choose which messages Alice wants to sign, and he knows the corresponding messages and the signatures. To overcome the above said attacks and to increase the security level, a hybrid approach is proposed by using Bilinear with Digital Signature to protect data stealing and alteration during data transmission. The MD5 is the hash algorithm that is used in the digital signature.

IV. EXPERIMENTAL SETUP

This research work describes the design of user authentication and secure data transmission in Wireless Sensor Networks for patient monitoring which aims a) to overcome mismanagement of treatment to patients due to altered reports. b) to maintain privacy of patients. In our system, patients, doctors and authorized relatives has to get registered with username , password and email ID from the Trust Authority(TA) in turn send a secret key to the registered mail ID, which is valid for 10 minutes. Person who registers and wants to access immediately can use the secret key received in mail. The registered user ID and password can be used in future to login and access. Whenever the user login with an interval of more than 10 minutes, a secret key has to be generated and submitted. Once, the data's are being submitted or uploaded by a registered user, the TA has to authenticate that the uploaded data are being sent by registered user and not altered by intruders.

V. PERFORMANCE ANALYSIS

In this paper, Bilinear pairing and digital signature are used for the user authentication. Key size, Key Generation Time and the Attacks of both Digital signature and bilinear pairing are compared with existing algorithm such as Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA) as tabulated below.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

TABLE-1 Various algorithms with Key size, Attacks and Key Generation Time

ALGORITHMS	KEY SIZE (bits)	ATTACKS	KEY GENERATION (sec)
Digital Signature Algorithm(DSA)	128	Key only attack , Known Message attack , Chosen Message attack , Adaptive Chosen Message attack	0.157
Bilinear Pairing	100	Impersonation, Replay attack, Online or Offline Password guessing attack, Stolen Verifier attack	0.132
Elliptic Curve Cryptography (ECC)	160	Known attack, Replay attack and Power analysis attack	0.210
Elliptic Curve Digital Signature Algorithm (ECDSA)	160	Impersonation, Stolen verifier, Denial of Service	0.161

A. Analysis of Key Size with various Algorithms:
The key size of various algorithms is tabulated below. And it is found that the key size of Bilinear Pairing algorithm is smallest among all other algorithm. Hence the key generation time for Bilinear algorithm is less. The Decryption time decreases, if the key size is large. Bigger key means longer decryption time means slower communication. Therefore, the smallest key size algorithm is chosen for improving the communication speed and to reduce the decryption time.

B. Analysis of attacks resisted with various Algorithms:
Though many attacks can occur in each algorithm, certain attacks are resisted by specific algorithms and are shown below. Bilinear pairing resists impersonation, replay attack, online or offline Password guessing attack, Stolen Verifier attack. Digital Signature algorithm resist Key only attack, Known Message attack, Chosen Message attack, Adaptive Chosen Message attack. Therefore the authentication improves by using both these algorithms.

1) Stolen-Verifier Attacks
This type of attacks involves stealing private information of users, such as ID and passwords, from verification tables in servers. If servers are not required to store verification tables, then this type of attacks is avoided.

2) Online Password Guessing Attacks
This type of attacks involves linking to a target computer directly and gaining legal access to an account through password guessing. During the login phase, the calculation of signature Sig and private parameter Upriv is done. An attacker must crack the Upriv to obtain the password. Thus, the attacker must solve the bilinear to crack the parameter, which is extremely difficult to achieve. In addition, the attacker must crack the password within certain period of time before being denied access. Therefore, online password guessing attacks are inapplicable.

3) Offline Password Guessing Attacks
This type of attacks involves finding the password of a goal user by intercepting data or through other security flaws. A specific program is employed to guess the password endlessly until the correct password is obtained or the cracking effort fails.
In the proposed system, even if an attacker intercepts Sig, because of the difficulty of the BDHP, the attacker would be unable to crack Upriv. Moreover, the attacker must solve the one-way hash function and guess the secret parameter a

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

to obtain the password. Therefore, this system is secure from offline password guessing attacks.

VI. CONCLUSION AND FUTURE ENHANCEMENT

Although there are many strategies to act against the security attack still an upgrade in the technology is needed. The attacks act against the security goals of the secure communication. Measures need to be taken to maintain the data integrity and authenticity. Cryptographic and techniques could be used to strengthen the network against any kind of malicious activity. By using Bilinear Pairing, replay, online or offline password guessing, and stolen- verifier attacks are avoided. By using Digital signature, Key only attack , Known Message attack , Chosen Message attack , Adaptive Chosen Message attack can be resisted. But, by using Bilinear Pairing and Digital Signature, the Related Key attack, Meet-in-the-Middle attack, Chosen input attack, Known Plaintext attack and Brute force attack are also avoided. Therefore, the authentication is improved by using both Bilinear Pairing and Digital Signature. Since, the key size is less, the key generation time is minimum, so the computational cost is reduced. Further, to prevent information and communication systems from illegal delivery and modification, message authentication and identification is examined through certified mechanisms. The messages transmitted from the sensor nodes over a wireless sensor networks is authenticated by the receiver. In future, the above mentioned defensive techniques need to be made stronger so as to safeguard the network during data transmission.

REFERENCES

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary,"Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, and Pervasive Computing, 2006.
[2] Jiguo Li ,Yuyan Guo ,Qihong Yu ,Yang Lu ,Yichen Zhang ,Futai Zhang ," Continuous leakage-resilient certificate-based encryption", Elsevier Journal on Information Sciences , 355–356 (2016) 1–14.
[3] Hongwei Li, Member, IEEE, Rongxing Lu, Member, IEEE, Liang Zhou, Member, IEEE," An Efficient Merkle-Tree-Based Authentication Scheme", IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2, JUNE 2014.
[4]L.F.Carvalho, G.Fernandes Jr,M.V.O.deAssis, J.J.P.C.Rodrigues, M.LemesProençaJr, "Digital signature of network segment for healthcare environments support", Elsevier Masson Journal on Healthcom , IRBM 35 ,2014, p 299–309.
[5] Thulasi Goriparthi , Manik Lal Das ,Ashutosh Saxena ,
"An improved bilinear pairing based remote user authentication scheme", Elsevier Journal of Computer Standards and Interfaces, 31 (2014) 181–185.
[6] Saru Kumari , Muhammad Khurram Khan , Mohammed Atiquzzaman," User authentication schemes for wireless sensor networks: A review", Elsevier Journal on Adhoc Networks, (2015) 159–194.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 16, 2017 ISSN: 2348-6600
Reference ID: IJCS-232 PAGE NO: 1445-1453
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

[7] Joselin.J ,S.J.Brintha ,V. Magesh Babu," Role of Digital Signature in Network Security and Cryptography", Elsevier Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, p 893-895.