Journal of Nuclear Energy Science & Power Generation Technology

REVIEW ARTICLE A SCITECHNOL JOURNAL

Enhancing Security in Wireless Sensor Networks

Prasanna Mishra[1]*, B. Nivedetha[2]

[1]*Department of Automobile Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India*

[2]*Department of Electrical and Electronics Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India*

***Corresponding author:** Prasanna Mishra, Department of Automobile Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India, Tel: 9490303888; E-mail: prasannamishra234@gmail.com

Received date: 25 February, 2022, Manuscript No. JNPGT-22-45683;
Editor assigned date: 01 March, 2022, PreQC No. JNPGT-22-45683(PQ);
Reviewed date: 14 March, 2022, QC No. JNPGT-22-45683;
Revised date: 21 March, 2022, Manuscript No. JNPGT-22-45683(R);
Published date: 24 March, 2022, DOI: 10.4172/2325-9809.1000259

Abstract

Authentication, confidentiality, integrity and non-repudiation are the key factors of security. They must be incorporated in order to protect data and information. All the data must be protected from intruders and hackers. If there is no proper security then the data can be stolen or eavesdropped easily by the intruders. To avoid this eavesdropping security factors should be enhanced to an additional level. Single factor authentication is not very safe since only password acts as the protection, it can be intruded. Two factor authentication is the password and one-time password which changes frequently, which is better than single factor but is also less secure. Hence three factor authentication is done with the fingerprint matching technique. It employs as an additional layer of security. The minutiae extraction is used and the better match is found. Thereby, the security can be enhanced in wireless sensor networks.

Keywords: Fingerprint; Wireless; Sensor networks; Extraction

Introduction

Cryptography is the science of information and security. It is fundamentally the science that incorporates mathematical logic to keep the information secure. It enables to securely store sensitive information or transmit information securely through insecure networks to keep it from being hacked. During authentication process, the identity of the user is verified to protect from any attacks [1]. Without authentication, any user with network access can use available tools to forge and impersonate others. A user needs login name and password for accounts that are authenticated from the server. Confidentiality means the assurance that only authorized users can read or use confidential information. Without confidentiality, anyone with network access can use available tools to eavesdrop. If privacy or confidentiality is not guaranteed, intruders could steal information. Integrity ensures that the original information is not altered or corrupted [2]. If the system fails to maintain the security aspect in integrity, then some user may modify information or might become corrupted. This alteration could sometimes be undetected. Non-repudiation indicates that the sender is for the sent message. If non-repudiation is not maintained, then someone will communicate and later either deny the communication entirely or claim that it occurred at a different time, or even deny receiving any piece of information [3].

Literature Review

Das proposed a secure and robust scheme that uses collision resistant one way hash function. Since the existing methods are vulnerable to privileged insider attack. It also lacks proper authentication and updation. This scheme provides pre-deployment of sensor nodes, Registration, login, authentication, key agreement, password, biometric update and dynamic node addition. It uses fuzzy extractor. It is resistant to privileged insider attack, online and offline password and biometric key guessing attack, Man-in-the-middle attack, tracing attack, stolen-verifier attack and forgery attack [4]. It ensures user anonymity and unlinkability. Li, et al. investigated the secure and robust temporal credential-based three factor authentication which does not provide session key agreement after mutual authentication. Three factor user authentication method with key agreement is designed to provide more security using biometrics. Passwords and tokens are commonly used but they might be forgotten and stolen [5]. Attackers can perform series of attacks such as updating user's password and impersonating legal user. Attackers might eavesdrop, intercept, delete and interpolate transmitted messages in insecure channel. The proposed scheme supports session key agreement between user and server after authentication process. It provides security of secret key, session key agreement and security, proper mutual authentication and also better functionality and performance. It also resists many attacks and ensures robust security. Fuzzy extractor is used for biometric verification and for security one way hash function is used. This scheme overcomes security weaknesses and provides session key agreement [6].

Jiang considered prolonged chaotic map provide three factor security and oppose various attacks. It also fails to preserve biometric template privacy. The process of password verification is invalid. Even if input identity and password are wrong, user can pass password verification, vulnerable to attacks. The proposed scheme resists several unknown attacks and provides mutual authentication using Burrows-Abadi-Needham (BAN) logic. It preserves biometric template privacy by employing fuzzy verifier and extractor. To fulfil local password verification fuzzy verifier is adopted. It supports authentication proof using BAN logic [7]. It helps in resisting replay attacks, modification attacks, server impersonation attack, denial of service attack. It provides secure channel, mutual authentication, forward secrecy, intractability. The computational cost is comparatively less. Wu proposed an novel three factor user authentication scheme for enhancing security. Legal user retrieving information should be based on mutual authentication. It considered secure and robust scheme which lacks user anonymity and strong security. In the proposed scheme sensors are collecting live data and information transferred to nearby gateway node which comprises of strong computing power. The user gets information by communicating with gateway node and decisions and activities are done. Hence common communication channel becomes insecure [8]. Only if the authentication process is passed then only the user becomes legal. The user and sensor builds common session key based on Elliptic Curve Cryptosystem (ECC). Since different collection of biometrics leads to different results Fuzzy extractor is used. It is resistant to many attacks like Insider attack, known key attack and ensures session key construction. On comparing, it is time consuming since ECC is employed. But time cost on gateway node is better and only one private key in gateway node [9].

Amin developed anonymity preserving three factor authenticated key exchange protocol. In existing methods there are issues like it is vulnerable to known session specific temporary information attack, password guessing attack and cannot preserve anonymity. The secret key for gateway node is insecure. The proposed method overcomes the issues and provides additional security attributes such as identity change and smartcard revocation. The Bio-hashing operation is employed. This scheme detects unauthorized login, achieves session key verification property, secure against attacks and preserves mutual authentication. It uses hash functions which are lightweight when compared to other techniques. This is secure against active and passive attacks. Network lifetime is prolonged by reducing energy consumption.

Objective of work

The main objective is to provide security in Wireless Sensor Networks. Authentication, Integrity, Confidentiality and Non-repudiation must be employed to ensure security. Authentication is done with the aid of three factors such as password, one-time password and fingerprint [10].

Project Description

Single factor authentication

In Single-Factor Authentication (SFA) process, only one credential of user is used for securing the network access or internet that the party asking access. Mostly, SFA is a password which is used for authentication. Password based security depends on system administrator or user who creates the account. A strong password has to be created to guarantee that only authorized users login. The issues with SFA are,

- Usage of single password increases the chances of password vulnerability so that intruders can easily hack the password.
- A hacker with correct knowledge of username can use specifically designed software to try to guess the password.
- With the updated speed of CPU's, even brute force attacks are also probable.

Two factor authentication

Two-Factor Authentication (2FA) improves the access security by using two different factors of each user. The factors can be something you recollect - like a user name and password, and something you own - like a card to authenticate request. This authentication method secures user network from various attacks like brute-force attacks and phishing. The problems with 2FA are,

- There is no certainty that authentication factors will be available when it is needed. Typically, user will be locked out of the account after one mistake is made.
- It is intended to keep hackers out of the account, but the vice versa can happen. Hackers can set up or reconfigure two-factor authentication to keep user out of their own accounts.

Three factor authentication

Three Factor Authentication (3FA) is used because it is better than single and two factor authentication. It provides extra layer of security, prevents from eavesdropping and it also prevents from attacks. The three factors are something you know-password, something you have-smart phone application, something you are- fingerprint. The factors are also known as, Knowledge factor, Possession factor and Inference factor [11].

Two factor authentication in desktop

Two factor authentication is vital because it enhances and additional layer of security. After implementing two-factor authentication, intruders cannot gain access to devices easily. It is very easy to create two factor key with Linux, so that user cannot log into the console or desktop without having the authentication code associated with that machine. The process of setting this up on Ubuntu Server 16.04 is done. If the set up is completed, user will gain access to the machine only by using the third-party generated codes. Every time if a user wants to log in, then user will be in need of either smart phone or the emergency codes. The requirements for this two factor authentication are Linux operating system and Google authenticator application in the smart phone [12].

Desktop login by authentication

To add an extra layer of security to Linux machines this two factor authentication is setup. Without the verification code, user will not be able to log into newly configured machine. To login in to desktop user must know two factors. First the password must be known then the one-time password which appears in the Google authenticator must be known. To be aware of the one-time password the user must always have the Google authenticator application in the smart phone. Only after completing the two step verification the user can login to the desktop.

Fingerprint recognition

A fingerprint pattern is made up of unique ridges and valleys on the individual finger. A ridge is a single curve section and this involves a lot of computation valley is the area between two adjacent ridges. The ridges are the dark areas of the fingerprint and white area between them is known as valleys. The physiological characteristics of user fingerprint are vital for verification since it will be unique for every individual. Fingerprint recognition is the most commonly used biometric technique in automatic identification. The fingerprint recognition will enhance the security; it will act as the additional layer of security. The fingerprint matching systems are based on four types. They are gray scale image, phase image, skeleton image and minutiae. The minutiae based representation has become most popular scheme because of its distinctiveness and compatibility. In fingerprint identification system, the captured fingerprint image needs to be matched with the stored fingerprint templates of every user in the database. This produces increased level of computation and search overhead. To reduce this, the minutiae features are extracted and match is checked with the input fingerprint image. The fingerprint matching is done with the aid of image processing. The matching of fingerprint is defined as finding degree of match between the input image and the fingerprint feature set. Initially one input image is given and the match is checked with the next input image. The flowchart below depicts the process followed in minutiae extraction.

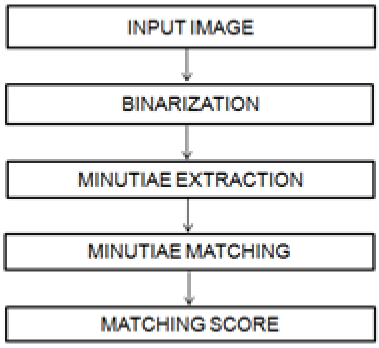


Figure 1: Minutiae flowchart.

Algorithm Development

Terminal window in Ubuntu

The terminal window in Linux OS is helpful for the two factor authentication setup. The Linux operating system is generally a command based OS. For every single operation they are based on commands. For instance, even to access a file, the respected command should be given; it is not like Graphical User Interface operating system [13].

Authentication in terminal window

Initially the terminal window is launched with which the Google authenticator application can be installed. The command used to install is “sudo apt-get install libpam-Google-authenticator” in which sudo command allows the user to run programs with the security privileges of another user. The command “apt-get” is used to retrieve the information and packages from the sources for installation, updation. Advanced packaging tool is the expansion of apt. “Libpam” is set of shared libraries which are used to dynamically authenticate a user to applications in Linux machines. Before installation it enquires for the password. Then the application has been installed. Modifications should be made to the lightdm so the following command “sudonano /etc/pam.d/lightdm” should be issued in the terminal window. The command “etc” contains the configuration files to run all the programs in the Linux machine. The lightdm indicates the display manager that is running in Ubuntu 16.04. The command “authrequiredpam_google_authenticator.so nullok” will be appended in the lightdm file. Then these changes should be updated to the lightdm file. It should be saved with the updated changes to the lightdm file to setup the authentication. Then the Google authenticator application starts running. It asks the user if the tokens should be time based and accordingly it automatically generates a QR code. The QR code should be scanned with the smart phone and the application will generate the one time password. In parallel the terminal will have a secret key, verification code and emergency scratch codes generated, and these keys can be used if there are any issues in login [14].

QR code generation

QR codes are machine readable code consisting of an array of black and white squares used for storing data or information. QR code stands for Quick Response code. Both Barcode and QR code are similar but the difference is that QR code is two-dimensional meaning it comprises of data in both vertical and horizontal directions. The QR code is generated in the terminal window with which the authentication takes place. The code that is generated is a random code.

Simulation Results

The two factor authentication has been configured in the Linux operating system in version 16.04. Initially the Google authenticator must be installed. After installation a QR code will be generated. The QR code must be scanned with the aid of smart phone then the verification code will be generated in smart phone which will be time based.

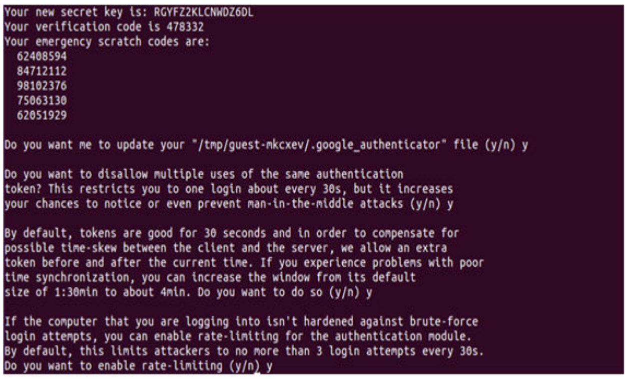
The token generated is one-time password that changes for every 30 seconds. QR code in the terminal window which should be scanned in the smart phone.

The Figure 3 displays the secret key, verification code and scratch codes which can be used for emergency purpose in case of no mobile phone. The Figure 4 depicts the first step of authentication that is something user knows password [15].

The figure 5 represents the second step authentication factor that is something the user has- smart phone. Only if both the factors are authenticated the user can login to the desktop.

In the Figure 6, the input fingerprint image is enhanced, false minutiae are filtered and minutiae are found. The threshold is set to find the accurate match. The match can be found by the matched fingerprint which will be displayed after the computation of similarity.

Figure 2: Generation of QR code.



```
Your new secret key is: RGYFZ2KLCNWDZ6DL
Your verification code is 478332
Your emergency scratch codes are:
  62408594
  84712112
  98102376
  75063130
  62051929

Do you want me to update your "/tmp/guest-mkcxev/.google_authenticator" file (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
size of 1:30min to about 4min. Do you want to do so (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting (y/n) y
```

Figure 3: Key generation.

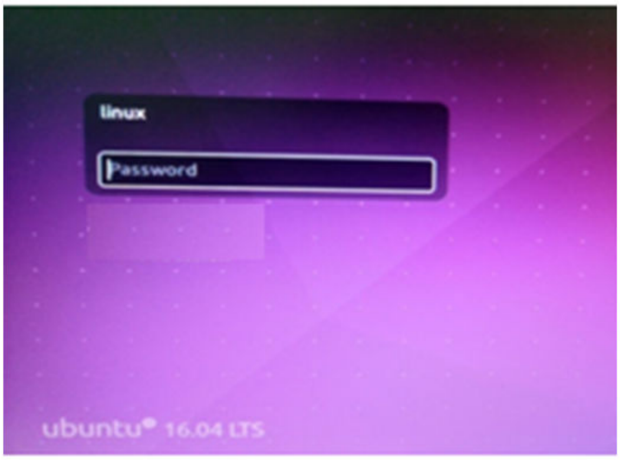


Figure 4: Password authentication.

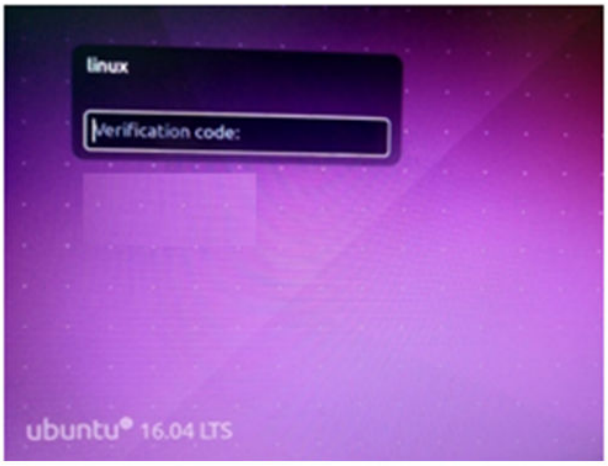


Figure 5: Verification code.

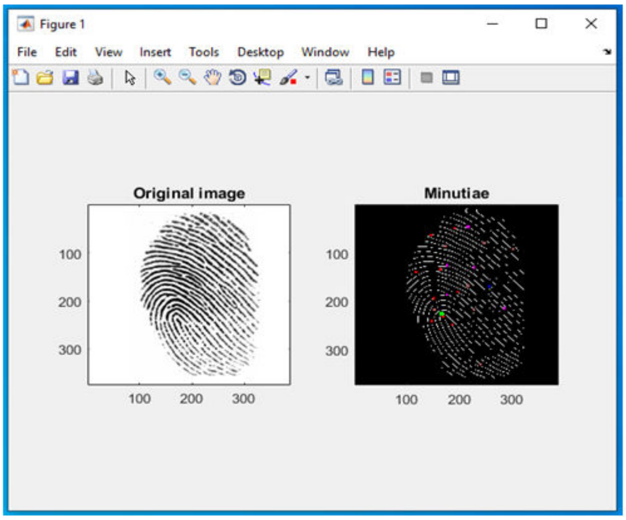
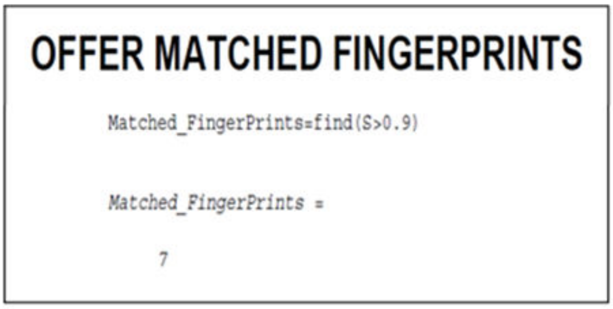


Figure 6: Minutiae extraction of image.



OFFER MATCHED FINGERPRINTS

```
Matched_FingerPrints=find(S>0.9)

Matched_FingerPrints =

     7
```

Figure 7: Matching of fingerprint.

Conclusion

In present days, security plays a vital role in all aspects like banking sectors, military, medical field and other applications. The multifactor authentication can be implemented to ensure security. The obtained output provides security to certain level with the help of three factors. In this case, the users can protect their data and safeguard it without the data being eavesdropped or attacked by intruders. The minutiae feature extraction is used for the fingerprint matching and the match is found.

Future Enhancement

The authentication factors can be extended by adding any other inherence factors like iris recognition and possession factor in order to improve the security features.

References

1. Das AK (2016) A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-peer Netw Appl 9: 223-244.
2. Li X, Niu J, Wang Z, Chen C (2014) Applying biometrics to design three-factor remote user authentication scheme with key agreement. Secur Commun Netw 7: 1488-1497.
3. Jiang Q, Wei F, Fu S, Ma J, Li G, et al. (2016) Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy. Nonlinear Dynam 83: 2085-2101.
4. Wu F, Xu L, Kumari S, Li X (2018) An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Netw Appl 11: 1-20.
5. Amin R, Islam SH, Biswas GP, Khan MK, Leng L, et al. (2016) Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput Netw 101: 42-62.
6. Althobaiti O, Al-Rodhaan M, Al-Dhelaan A (2013) An efficient biometric authentication protocol for wireless sensor networks. Int J Distrib Sensor Netw 9: 407971.
7. Chen TH, Shih WK (2010) A robust mutual authentication protocol for wireless sensor networks. ETRI J 32: 704-712.
8. Nivedetha B, Vennila I (2020) FFBKS: Fuzzy fingerprint biometric key based security schema for wireless sensor networks. Comput Commun 150: 94-102.
9. Das ML (2009) Two-factor user authentication in wireless sensor networks. IEEE Transact Wireless Commun 8: 1086-1090.

10. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J Comput 38: 97-139.
11. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Transact Informat Theory 29: 198-208.
12. Fan CI, Lin YH (2009) Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Transact Informat Foren Secur 4: 933-945.
13. Guo P, Wang J, Geng XH, Kim CS, Kim JU (2014) A variable threshold-value authentication architecture for wireless mesh networks. J Intern Technol 15: 929-935.
14. Yuan JJ (2014) An enhanced two-factor user authentication in wireless sensor networks. Telecommun Syst 55: 105-113.
15. Khan MK, Alghathbar K (2010) Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks’. Sensors 10: 2450-2459.