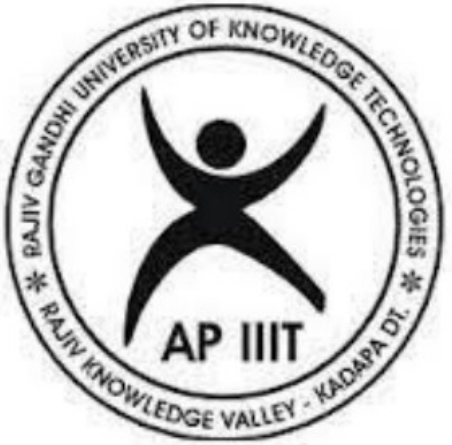
SECURE AND FLEXIBLE FOUR FACTOR MUTUAL AUTHENTICATION FOR WBAN

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING



Rajiv Gandhi University of Knowledge Technologies

R.K.VALLEY

Submitted by

Devangam Ambe Mahesh	R170527	G Sneha	R170614
Dugganaboina Gowtham Kumar	R170523	B Poojitha	R170621
Shaik Enus	R170585	K Safiya	R170610
Shaik Amer	R170862	Palagiri Gowhathi Raj	R170611
M Siva Kumar	R170793	Shaik Afreed Hussain	R170670
Kusam Tejaswar Reddy	R170728	Shaik Afrin Begum	R170680

Under the Esteemed guidance of

T.Sandeep Kumar Reddy Asst.Prof

Computer Science Department

RGUKT RK Valley

R17 Batch (2017 - 2023)

DECLARATION

We hereby declare that the report of the B.Tech Major Project Work entitled " **SECURE AND FLEXIBLE FOUR FACTOR MUTUAL AUTHENTICATION FOR WBAN** " which is being submitted to Rajiv Gandhi University of Knowledge Technologies, RK Valley, in partial fulfillment of the requirements for the award of Degree of Bachelor of Technology in Computer Science and Engineering, is a bonafide report of the work carried out by us. The material contained in this report has not been submitted to any university or institution for award of any degree.

By all the team members

Dept. Of Computer Science and Engineering.

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE AND TECHNOLOGIES

RGUKT

(A.P.Government Act 18 of 2008)

IIIT RK VALLEY, RGUKT-AP

Department of Computer Science and Engineering

CERTIFICATE FOR PROJECT COMPLETION

This is certify that the project entitled submitted by Devangam Ambe Mahesh(R170527), Dugganaboina Gowtham Kumar (R170523),Shaik Enus(R170585),Shaik Amer(R170862), M Siva Kumar(R170793),Kusam Tejaswar Reddy (R170728),Shaik Afreed Hussain(R170670), Palagiri Gowhathi Raj(R170611),K Safiya (R170610),Shaik Afrin Begum(R170680),B Poojitha (R170621),G Sneha(R170614),under our guidance and supervision for the partial fulfillment for the Degree Bachelor of Technology in Computer Science and Engineering during the academic year 2022-2023 at AP IIIT RGUKT RK VALLEY. To the best of my knowledge,the result embodied in this dissertation work have not been submitted to any University or Institute for the award of any degree or diploma.

Project Internal Guide

T.Sandeep Kumar Reddy

Assistant Professor

IIIT,RGUKT-AP

Head of the Department

Ratna Kumari Challa

HOD of CSE

IIIT,RGUKT-AP

INDEX

1. Abstract

2. Introduction

3. Authentication

4. Security Attacks and their services

5. Efficiency Evaluation Of Proposed Scheme In Two-Factor Authentication

6 Conclusion

Abstract

Wireless body area networks (WBAN) is a novel paradigm that is gaining popularity in a scenario of current wireless communication systems. It plays an essential role in health care applications like remote monitoring of health data. For instance, the crucial and confidential data about the condition of the patient's physical healthcan be gathered and transferred through WBAN.Therefore, authentication and session key-agreements are integral security concerns for wearable sensors in WBAN. Moreover, as the wearable devices are resource-constraints, there is a need to develop a lightweight protocol to ensure authenticity, confidentiality, andintegrity of the information. Li et al. presented an anonymous mutual authentication protocol to establish a session-key among wearable sensor nodes and the local hub node. However, after an in-depth analysis,we found that their scheme is susceptible to an intermediate node capture attack, and sensor node/hubnode impersonation with intermediate node capture attacks. The scheme also does not provide anonymity with unlinkable sessions. This paper proposes a new anonymous mutual authentication and key agreement protocol in WBAN to overcome the security weaknesses in Li et al.'s protocol. The proposed protocol uses only basic symmetric cryptosystems like simple XOR and cryptographic hash functions; hence, it is efficient and light weight. The validity and the correctness of the proposed protocol are evaluated using BAN-Logic and the broadly accepted AVISPA tool. The performance comparison of the proposed protocol with the existing related protocols shows the efficiency regarding communication computational complexities.Hence, it is suitable to be used in real-life applications.

Introduction:

- The advances in microelectronics and embedded technologies resulted in the advent of miniature and ultra-low power sensors or wearable devices with the ability to sense, process and transmit.
- A Wireless Body Area Network (WBAN) is formed by various wearable sensors that are situated in the body of patient, where the nodes are connected via wireless communication technologies.
- WBAN can be used to monitor and track physical conditions of patients without reducing the user's comfort by using an Intranet or Internet.
- WBANs can provide many applications combine with cloud computing technology, such as vital signmonitoring, home care monitoring, clinical monitoring, and sportsperson health condition monitoring .
- Two Factor authentication scheme contains a multi-hop centralized architecture, where a special central node, called local server or hub node is invloved in this architecure and all the mentioned information of sensor nodes would be sent to it.

- There are 3 types of nodes.
- Sensor nodes- Attached to patient and records information
- First level nodes- takes information and send to hub node.
- Hub Node- Receives and stores the information.
- In Four Factor authenticaiton and two factor authentication which contains gateway in middle, WBAN consists of a set of sensors deployed around body along with that a gateway node for controlling and monitoring the sensors and a set of users.
- However the sensor nodes may include a coordinator node among them.
- Gateway aggregates the received data and send it to the concerned authority, such as doctors,family etc.

Authentication

- In Every Prosposed scheme ,There are 3 common phases :
  1) Initialization
     - Parameters are initialized for system participants by SA
  2) Registration
     - Users/Nodes gets registered by SA as a legal entity
  3) Authentication
     - Principals mutually authenticate each other to gain access to system resources

- In Addition to the 3 phases mentioned previously,There is an extra phase in 4-factor Mutual Authentication scheme proposed by Fotouhi,Bayat and Ashok Kumar.
- The 4^{th} Phase is known as “Password Change Phase”.
- In this phase,User can change the password if he wants to change the password.
- The User have to provide user id and password as input in this phase,to change the password.

Security Attacks and their services:

- The messages exchanged in the WBAN contain vital ans sensitive information about physical conditions of patients, and this information is important for patient's privacy.
- Security attacks are the actions that cause affect to the both authentication and key agreement for the transmission scheme.
- Security Services are the actions that counter or prevent the security attacks by providing all security requirements required to them.
- Three authentication schemes sustains so many attacks and also can't provide service again some security attacks.
- There are so many attacks which can be sustained by these two and four factor authentication schemes such as providing anonymity,sensor node impersation attack,replay attack,stolen verifier attacks,sensor node capture attacks,Man in the middle attacks etc.

Security Attack/Security Service	Two Factor Authentication	Two Factor Authentication with Gateway in middle
Mutual Authentication	Yes	Yes
Perfect Forward Secrecy	Yes	Yes
Anonymity and Untracebility	Yes	Yes
Sensor node impersonation Attack	Yes	No
Sensor Node Capture Attack	Yes	Yes

Security Attack/Security Service	Two Factor Authentication	Two Factor Authentication with Gateway in middle
Replay Attack	Yes	No
Privileged Insider Attack	No	Yes
Man in the middle Attack	Yes	No
Hub Node Spoofing Attack	Yes	No
Gateway Impersonation attack	No	Yes

Security Attack/Security Service	Two Factor Authentication	Two Factor Authentication with Gateway in middle
Session Key Disclosure Attack	Yes	Yes
Username and Pasword Guessing Attack	No	Yes
Stolen Device Attack	Yes	No

EFFICIENCY EVALUATION OF PROPOSED SCHEME IN TWO-FACTOR AUTHENTICATION

Efficiency evaluation of proposed scheme in two fator authentication

In this section we concretly evaluate the efficiency of proposed scheme. We evaluate the storage requirements, the computation cost, the energy consumption and the communication overheads.

Storage requirements

In our scheme, the hub node is required to store its own master secret key k_{HN} as well as id'_N of the registered first level sensor nodes. On the other hand, each second level sensor node is required to store the tuple $<id_N , a_N , b_N >$, in addition to the session key k_s . For a first level node, it is required to store also id N which is assumed short (16 bits). We use SHA-1 as an example of hash function, and the output of SHA-1 is 160 bits. By applying these settings, then $| id_N | = | a_N | = | b_N | = | k_s | = | k_{HN} | = 160 | = 16$ bits. The total storage required by HN is bits, while $| id_N(16 m + 160)$ bits, where m is the number of registered first level sensor nodes. Each second level node N is required to store 640 bits.

Computation cost

Our scheme uses two operations, i.e. hash function and XOR operation. Let t_h and t_{xor} to be the computation time of one hash invocation and one XOR operation, respectively. Considering the authentication phase. The hub node HN performs 5 hash invocations and 11 XOR operations. These total $5t_h + 11t_{xor}$. On the other hand, the sensor node N performs 3 hash invocations and 6 XOR operations. These total $3t_h + 6_{xor}$. The computation time of XOR operation is very trivial and can be ignored assuming $t_{xor} \approx 0$. Therefore, the computation cost required by HN becomes $5t_h + 11t_{xor} \approx 5t_h$. The computation cost of the sensor node N becomes $3t_h + 6t_{xor} \approx 3t_h$.

Storage and computation cost of our scheme

Node	Storage cost (in bits)	Computation cost
N	640	$3t_h + 6t_{xor} \approx 3t_h$
HN	16m + 160	$5t_h + 11t_{xor} \approx 5t_h$

Conclusion

- Proposed scheme of two factor authentication is a lightweight authentication scheme for two-hop centralized WBAN, and it provides anonymous and unlinkable features for wearable sensors while achieving the mutual authentication between wearable sensors and hub node. Our scheme just need to execute hash operations and XOR operations and it is more efficient than previously related schemes. Specifically, the sensor node and the hub node are just need to perform three and five hash operations respectively.
- In this scheme , privileged insider attack,Gateway impersonation attack,Username and Pasword Guessing Attack .These attacks are need to be improved with further implementation in algorithms..
- Proposed scheme of two factor authentication(includes gateway) provides perfect forward secrecy and other security requirements like resistance to key compromise impersonation attack and known session-specific temporary information attack.

- In this scheme,Stolen Device Attack,Man in the middle Attack,Hub Node Spoofing Attack,Sensor node impersonation Attack are need to be improved and these need to be implemented with further modification of algorithms.
- We have verified the system’s security through the AVISPA simulation tool. Its performance evaluation shows that it can fulfill the desired security properties with the reduced communication, computation, and storage overheads,proving that it meets computation cost efficiency requirements and suitability for real-life applications of WBANs.
- The results showed that proposed scheme is significantly more secure and efficient to be implemented in health-care environments but inorder to maintain more security with many attacks we need to move to four factor authentication.
- In the future, we will continue to explore these security problems of WBAN, and design wearable sensors applicable security solutions.

ACKNOWLEDGEMENT

We would like to express my sincere gratitude to **Mr T.Sandeep Kumar Reddy Asst.Professor** ,my project internal guide for valuable suggestions and keen interest through out the progress of my course of research

We are grateful to **Mrs.CH.Ratna Kumari**, HOD CSE, for providing excellent computing facilities a congenial atmosphere for progressing with my project.

At the outset, We would like to thank **Rajiv Gandhi University of Knowledge Technologies(RGUKT) RK Valley** for providing all the necessary resources and support for the successful completion of our course work.