AN ANONYMOUS MUTUAL AUTHENTICATION MECHANISM FOR WEARABLE SENSORS IN THREE-TIER MOBILE HEALTHCARE SYSTEMS

A. HEMLATHADHEVI[1], D. R. THIRUPURASUNDARI[2], C. RAMESH KUMAR[3] *,
G. NIRMALAR[4]
[1]Department of Computer Science and Engineering, Panimalar Engineering college, Chennai, TamilNadu, India.
[2]Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu.
[3] *School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.
[4]Department of Computer Science and Engineering, R.M.D. Engineering College, Chennai, TamilNadu, India.
E-mail: [1]hemlathadhevi@gmail.com, [2]tpsdrlagok@gmail.com, [3]gns.cse@rmd.ac.in, [4] *toramesh83@gmail.com

ABSTRACT

In light of the openness and mobility of wireless communication, Mobile Healthcare Systems are vulnerable to a wide range of threats, which considerably reduces their value and hinders their widespread implementation. Patients and medical personnel can be linked to their actions by attackers and criminals, even if they don't realize the context of the data they're transmitting, by simple eavesdropping. All levels of the mHealth ecosystem are affected by these flaws. This research proposes an anonymous mutual authentication mechanism for wearable sensors in three-tier mobile healthcare systems. The HSP medical server, controller nodes, and the anonymous authentication nodes of mobile users are all supported. It also makes it possible for mobile users and controller nodes to exchange authentication information anonymously. The controller nodes and the wearable body sensors are anonymously authenticated with the help of this method of authentication. In order to ensure the security of our protocols, we do extensive formal demonstrations and informal conversations about security features, prospective attacks, and responses. Simulated outcomes indicate that our strategy is safe and meets all of the required privacy and authentication requirements.

Keywords: *Wearable Sensors, Anonymity, Authentication, Healthcare, Security, Wireless Body Sensor Networks.*

1. INTRODUCTION

In computers and communications, the Internet of Things (IoT) is definitely a big technical advance. In 1999, Kevin Ashton coined the term Internet of Things (IoT) for supply chain management. He described the Internet of Things (IoT) as a network of radio-frequency identification (RFID)-enabled items that can communicate with each other. The Internet of Things (IoT) has been characterized in several ways in the academic literature. Using established protocols, the RFID group defines IoT as a collection of networked devices that can be identified only by their RFID tags [1].

Wireless connectivity and cloud computing have enhanced healthcare services in the modern day. With the use of wireless sensor networks, mHealth solutions may be designed that are efficient and effective in preventing or preventing the spread of disease and preparing for emergencies. The healthcare industry, on the other hand, is fast being improved through mobile networks, nanotechnology, wearable technologies, and widespread computerization. Acute care, primary care, and public health all benefit from the integration of these cutting-edge technology.

Physical sensors, microprocessors and RF devices were merged into a single micro-chip, resulting in extremely low-power, ultra-lightweight, and highly accurate monitoring sensor devices. Wireless technology is used to detect, process, and send crucial physiological signals via these sensor devices. With the use of an Intranet or the Internet, wireless body sensor networks (WBSN) may be used to watch and track the state of patients in both urban and rural regions, decreasing the chores of healthcare personnel, avoiding medical mistakes and enhancing patient comfort. [2].

As a result, patients' quality of life can be improved by using these systems, which allow remote acquisition and monitoring of physiological/vital data without interrupting their daily routine. Mobile Health (mHealth) systems are emerging as a result of the convergence of devices, technologies and networks in the development of the new telemedical and e-health systems, as well as a new age of Mobile Health (mHealth) systems. Long-term monitoring of a patient's health can be accomplished via a Wireless Body Sensor Network (WBSN). The monitoring of vital signs, home care, clinical monitoring, and the health condition of athletes are all important uses of WBSN. Figure 1 depicts the overall structure of a mobile health system.

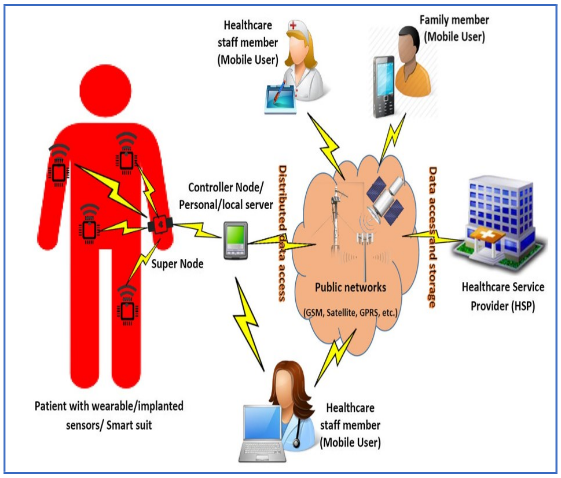

Figure 1: General architecture of a e-health system

Connected to the patient's body are small sensor nodes (wearable sensors). These tiny sensors, which can be worn or implanted, are used to accumulate vital information from the body of the patient. Using a special node called a super sensor node, which is likewise wearable, but with higher compute and storage capabilities than ordinary wearable sensors, this data is sent to the wearer's device. mHealth's initial layer is made up of small and large sensors connected in a star network structure. As a subnetwork of the mHealth network, the IntraBAN network is sometimes known as the first tier. It is this controller node, also known as a local server or gateway, that acts as an intermediary between the super sensor nodes and the controller node, which is the more powerful of the two [3].

The controller node in the third tier collects all patient data and transmits it to the medical server of the healthcare provider over public networks. A patient's electronic medical records can then be accessed by approved mobile clients/users (eg. physicians and nurses, emergency service personnel and family members) (EMRs). This can also be accomplished using public wireless networks or the Internet. To secure the data security and privacy communicated in a mHealth system, it is essential to protect patients' health-related information. Doctors' ability to perform precise diagnosis and treatments would be greatly harmed if the health data they get via mHealth networks is altered in any way.

Medical services in WBANs should be provided anonymously, i.e., physicians only need to know the patient's health information and therefore have no knowledge of the patient's personal information, including such his name or identification number. Since it can enable authentication mechanism among the client and the software platform and anonymously produce a session key for data encryption, practice shows that anonymous authentication technique is the most effective solution to such difficulties. Additionally, medical staff workers have the option to continue unidentified and their actions to the patient's medical data remain untethered [4].

Hackers and scofflaws may gain a great deal by linking the activities of a patient's sensors and healthcare workers without knowing the context of the supplied data. Medical personnel who have access to the controller node of a patient may interpret an increase in traffic as an indication of a potentially life-threatening medical condition, which might be used to motivate criminal behaviour (for example, cardiac arrest) against the patient. [5].

There are a variety of issues that must be faced when designing data security and privacy methods for mHealth, including how to better balance safety, economy, and pragmatism. Security methods in a WBAN must be as compact and cost-effective as feasible because of the limited resources of the sensor nodes. Keeping an eye out for practical considerations such as security vs. safety vs. usability is also a good idea. The access control systems ought to be context-aware and adaptable in order to enable authorised access to patients' data in time-sensitive situations such as emergency treatment [6].

2. LITERATURE SURVEY

Since the World Health Organization's research on ageing and disability predicted that most people worldwide will survive above the age of 60, life expectancy has increased. Chronic illnesses, impairments, and increased hospitalization are all more common in the ageing population. As predicted by the researchers, healthcare services delivery would be converted from hospital–home equilibrium in 2025, to homecare services in 2030, within a few decades. As a result of the technological change, patients now have access to a variety of new services such as remote vital sign monitoring and prescription management via telemedicine. m-health solutions for melanoma and several long-term illnesses including obesity and diabetes have been found to be acceptable and usable by patients [7].

Some studies focus on assisting diabetes patients with self-management, such as tracking their blood glucose levels and calculating their insulin needs. As a result, patients may monitor their calorie intake, measure their physical activity, and interact with others who can give crucial support using mobile phone applications. All of these elements work together to influence a person's way of life for the better and result in better health. An emerging area of study known as mIoT (the Internet of mHealth Things) has just emerged. Simple physiological signal detecting systems for blood pressure, oxygen intake, and body temperature were created by Sung et al. and merged in the cloud [8].

An IoT use for ophthalmology was presented in another study. Lens colour and blood flow sensor readings are transmitted through this model's glasses to indicate ocular hemorrhage. Every party to the connection can verify the legitimacy of the other parties using authentication schemes, which have been utilized in a variety of settings from single server environments to multi-server environments to wireless sensor networks. To authenticate a user, a password, a smart card, and biometrics can all be utilized. The plans are geared at the introduction of smart cards. The multi-server architecture targeted by these systems makes use of identity-based authentication.

Biometric-based remote verification is proposed, whereas password-based identification is proposed with many advancements. Several bidirectional authentication mechanism exchange mechanisms have been proposed for e-healthcare systems and WBANs. No matter how efficient, safe, and light these techniques may be, they do not consider anonymity and unlinkability [9]. The primary and secondary tiers of these systems are the only ones that take secure communication between entities in a third-tier subnetwork into account. Although the healthcare server's master secret key has been hacked, Khan and Kumari created a security mechanism in 2013 for better accessibility to the TMIS.

Using a random oracle model, Islam and Khan created an ECC-based two-factor signature scheme for TMIS, and they proved the reliability of their approach. Users can access TMIS services through a smartphone with the help of Siddiqui et al.'s three-factor authentication system. If you want to get access to a medical system, you can't utilize any of these methods. With the release of Sawant et al.'s architectural framework in 2014, a set of obstacles for designing high-quality patient-centric monitoring schemes was highlighted, as well as a few possible solutions. The schemes are designed to protect the extra-body communication between the WBAN client's smart portable device (hub) and the platform providers, such as the clinic, doctor, or hospital professionals [10].

With the use of a new certificateless signature (CLS) technique and a random oracle model that uses adaptive message selection, Liu and colleagues developed two optimization and light-weight authorization protocols that allow distant WBAN users to access healthcare services anonymously. For the WBAN application scenario, Liu et al. proposed two novel authorized key exchange protocols symmetric key encryption cryptosystem and established a layered network architecture with a two-hop network domain [11]. For large-scale WBANs, the certificateless anonymized secluded verification with revocation was suggested later by Xiong and Qin in 2015.

In order to provide a remote authentication method featuring non-repudiation, client confidentiality, key exchange resilience, and unlinkability for WBAN extra-body transmission, the ideas rely on certificate-less encryption. Even while these methods offer high levels of security, they are more closely associated with digital signatures than with authentication, and as a result, they are not well suited for use on mobile devices or with sensors of a small size. Just the third-tier entities, such as the AAL server (in our case, the HSP medical server) and the controller node, were the focus of the authentication strategy. However, the second tier of authentication between microcontroller nodes and body sensors was not considered in their study [12].

In order to offer an anonymous authentication method for the third tier alone, the schemes developed a method that only authenticates between the user and server. They didn't even think about using another kind of authentication. Since Li and colleagues recently introduced an unidentified mutual key agreement technique for wireless body area networks, the sensor nodes attached to the patient's body can authenticate and establish a session key in an unlinkable way by using their approach. Because the H S P healthcare server transmits data via public networks, it is vulnerable to a wide range of cyberattacks. Since open wireless networks like Zigbee or WiFi are used to communicate, this problem also applies among the administrative networks and the advanced sensor nodes [13]. An authentication scheme that can withstand a wide range of assaults is the primary objective of this research.

3. PROPOSED SYSTEM

The three main parts of the WBAN system are a collection of medical sensors, a cell phone (also known as a base station or sink), and a backend server. This is our network model. Patients' information is sent every 60 minutes to a backend server once mutual authentication between the cellular phone and a medical sensor node is performed. We've also built in a Trusted Third Party (TTP) to distribute and manage the network's public and private keys, including those of sensors, mobile devices, and the backend server.

When it comes to design, wired connection among sensor clusters and a base station is the best option. MITH and SMART are two examples of systems that use cables to communicate multiple commonly produced sensors to a PDA. It is impracticable and inhibits patient movement to distribute cables throughout the body, which is essential to an electronic health care (e-Health) system's success. WBAN provides the patient with the ability to move around while the design is being finalized. WBAN is mostly employed in the medical field, although it can also be used in non-medical settings.

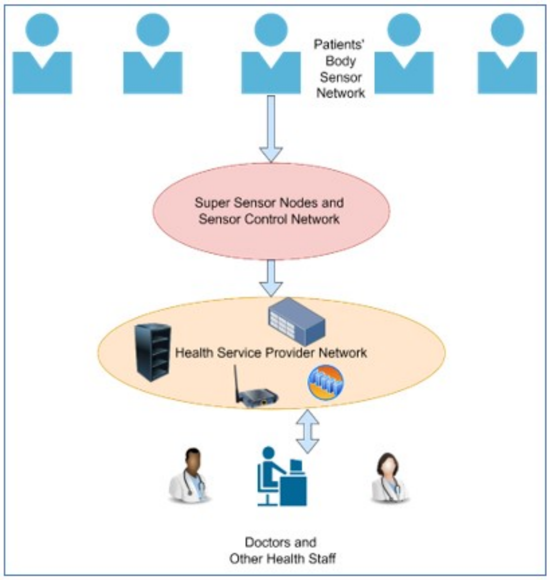
Patients' Body Sensor Network
Super Sensor Nodes and Sensor Control Network
Health Service Provider Network
Doctors and Other Health Staff

Figure 2: Proposed system architecture

Patients with age-related chronic conditions, such as heart attacks, high blood pressure, or diabetes, would benefit from a low-cost and practical method of remote monitoring through the implementation of WBAN in this field. Each sensor node that is implanted on a person's body has three primary functions: data endurance, contraction, and masking. Sensor nodes with their central station communicate via short-range wireless technology. A detailed summary of any of these things is provided below. Physiological signals can be monitored using a wide range of sensors in wearable biometrics (WBAN) in the Figure 2.

An electronic instrument can read the signals generated by sensors. These sensors connect the physical and electrical worlds since they may be worn on the body or implanted within the body. Patients wear on-body sensors, as the name implies, while those implanted inside the body are referred to as in-body or implantable sensors. Numerous sensor nodes that can be utilized in WBAN, including data rates, are summarized in the following table. To minimize the amount of data being communicated, the Analog-to-Digital Converter (ADC) often performs pre-processing on the signal being sampled.

It is proposed in this study that the sensor network and its linked mobile telephone in a WBAN be mutually authenticated, and the shared secret key generated between them. When used in this way, the mobile phone acts as a drain on the WBAN. It comprises four phases: startup, mutual authentication and key creation and encryption and decryption. Prior to deploying the network, a trustworthy Third Party distributes the public/private key to medical sensor network and cellular phones. Additional security measures include periodic key re-distribution and key regeneration. A huge prime number P and its primitive root G are also selected and distributed by the TTP to all sensors and the cell phone.

During the key creation process, the letters P and G are utilised last. In a WBAN, a sensor (SN) within the body and a sink (PH) on a mobile phone achieve mutual authentication. In order to join the network, a medical sensor node must submit a query message encrypted with PH's public key to register. It includes a sensor node identity, a random number produced by the sensor node, a random number, the sensor node's public key and a timestamp. The sensor's public key is used to encrypt a challenge message that the PH sends back in response to the add request. PH IDs are stored by the sensor node after receiving and decrypting a challenge message. These IDs will be used later in the authentication process. the identifier and timestamp from the issue message with those generated and sent in an add request message are compared to verify PH authenticity. ID and timestamp in encrypted messages, add permission and challenge, must match for the PH to be considered legitimate.

In response to the PH's challenge message, the sensor node sends a response message encrypted with the PH's public key and including the identical ID and timestamps generated by both parties. It then gets the answer message decrypted, checks the received unique id and timestamp against the ones in the challenge message, and then compares the results. The sensor node is authenticated by the PH if the following values are the same. As soon as the two parties have successfully verified their identities, they may now create a shared secret key. Operation Tts distributes a huge prime number P and a primitive origin G as indicated in the startup step. To begin, A and B are chosen at random by the sensor node and the mobile phone, respectively.

As a result, X is calculated by the sensor node as X=GA mod P and W is calculated by thePH as W=GB mod P The mobile phones sends W to the regulatory system after XoR ing it with this sensor's ID in order to overcome the Diffie-Hellman scheme attack problem. After XoR ing it with the PH's ID, the sensor node delivers X to the PH. As a result, R and R' are exchanged between the sensor node and PH. Both PH and the sensor node must XoR their acquired value according to their own ID in order to complete the Asymmetric cryptographic scenario and retrieve X and W. Accuracy of measurements at sensor nodes and at Phasors (PH). A Diffie-Hellman scenario continues, with nodes I and XB mod P calculating the same shared secret key S, while nodes I and XB mod P do the same on mobile phones.

```
Algorithm 1: Authentication for communication for super sensor node
Steps:
    1. Generate $S_{rand}$ which is a random number.
    2. Estimate server key $S_{key} = h(SN_{key}, SN_{tid}, SN_{id}, S_{rand})$
    3. Create hashed value using the hash function $SN_H = h(SN_{key}, SN_{id}, S_{key}, S_{rand})$
    4. $y = h(SN_{id}) \oplus S_{rand}$
    5. Calculate from control node information:
        a. Find the generated super node sensor id value as $SN_{tid}^* = a \oplus h(S_{key})$
        b. Estimate control node hash function component as $CN_H = h(S_{key}, SN_{tid}^*)$.
        c. Instead of $SN_{tid}$, use the newly generated id $SN_{tid}^*$.
        d. Regenerate the $S_{key}$ and keep it for future use.
```

Amplification and Filtering, compression, and advanced signal processing are all examples of pre-processing techniques. Pre-processing enables patients to only provide data that is absolutely necessary to their healthcare providers. This allows for more efficient use of resources, less power use, and real-time streaming. To match the ADC analogue full-scale range with bio signals, which are generally on the mV order, amplifiers must be used before the A/D conversion takes place. If an instrumentation amplifier is utilised, it will usually have a differential input. The elimination of distortion and aliases frequently necessitates filtering of sensor data at the sensor node. At the sensor nodes, data filtering reduces power usage by removing unnecessary information. Filtering techniques like FIR or moving average filtration could be used to the sampled data for further processing. Prior to transmission, it is also possible to examine the sampled data for duplicates and remove them. Wireless sensor networks (WSNs) and WBANs are using low-cost, battery-powered nodes in order to save money.

$$\frac{HSP \mid\equiv N \mid\equiv (N \xleftrightarrow{K_N, ID_N} HSP, t_N, r)}{HSP \mid\equiv N \mid\equiv (N \xleftrightarrow{K_N, ID_N} HSP)} \text{-----------------------------------} 1$$

In order to extend the operational lifespan of these nodes, it is necessary to use energy-efficient data collecting and aggregation methods. The application operating at the sink is sophisticated enough to derive the outcome by simulating actual data using the approximate replication approach, which was recently introduced to WSN. An adjustment and optimization method were used to make it possible to send just a portion of the data that was really sensed. Data screening in WSN may be automated using this method. Proposal approach was designed to find the optimal balance between computing and communication power, in order to reduce the total system's power consumption. Experimental results reveal that the recommended filtering approach saves a lot of energy when used to a real-world application. In the end, the pre-processed patient data reaches the base-station. This is the most energy-intensive but also the most difficult task.

Algorithm 2: Control node Authentication Process
Steps:

```
1. Establish the values of $SN_{ch}, SN_{tid}$ and $CN_{key}$ from the super sensor node as discussed in algorithm 1.
2. Calculate $SN_{id}^{*} = SN_{ch} \oplus h(SN_{tid}, CN_{key})$
3. Estimate $s^{*} = y \oplus h(SN_{id}^{*})$ and $SN_{key}^{*} = h(SN_{id}^{*}, CN_{key})$
4. Find the value of $s_{key}^{*} = h(SN_{key}^{*}, SN_{tid}, SN_{id}^{*}, s^{*})$
5. Compute $SN_{H}^{*} = h(SN_{key}^{*}, SN_{id}^{*}, s_{key}^{*}, s^{*})$
6. If $(SN_{H}^{*}$ equals $SN_{H})$
    a. Compute a fresh value of $SN_{tid}{}^{*}$
    b. Calculate
       $a = h(s_{key}^{*}) \oplus SN_{tid}{}^{*}$
7. Now $CN_{H} = h(s_{key}^{*}, SN_{tid}{}^{*})$
8. Find
   $SN_{ch}^{*} = SN_{id}^{*} \oplus h(SN_{tid}{}^{*}, CN_{key})$
```

Compute the session key for the control node $s_{key}^{*}\langle SN_{tid}, CN_{H}\rangle$

We must employ low power, short range wireless technologies since sensor nodes are battery driven. It is possible to use a variety of short-range wireless technologies, but each has its own set of obstacles. There are several short-range low-power techniques that may be utilised to communicate among sensor network and base stations. In addition, it discusses numerous WBAN security, MAC layer, QoS, and Physical layer concerns. Our system has four essential components. Setup or initialization of the system preferences and registrations of other entities are handled by the H S P medical server. The patient's vital signs are collected by tiny wearable or implanted sensors and sent to the super sensor nodes (SNs). The HSP medical servers receive patient data from the SNs via the controller nodes (CNs). The resources of these sensors, while greater than those of SNs, are nevertheless restricted. Patients' electronic medical records (EMRs) can only be accessed by approved mobile clients/users.

The trustworthiness of the HSP is regarded as high. Trust in the HSP comes as a result of it being responsible for creating all of the system's hidden settings. It's possible for any other entity to act maliciously. In the third tier, the controller nodes (CNs) are used to interact with the HSP medical server, and in the second tier, they are used to connect with the body sensors via the wearable super nodes (SNs). There are two levels of communication between the wearable super sensors (SNs) and the controller nodes. The first level of communication is with the wearable/implanted sensor nodes, and the second level of communication is with the controller nodes. It is possible for an outsider enemy to eavesdrop on all of the system's communication lines. Records and plays back messages for any recipient.

Patients' essential medical situations are linked to specific nodes via the transmission of signals. Messages that are intercepted can be decomposed and reassembled as a new message and resent to any entity. They Use the stolen or leaked secret keys to decrypt and decode communications. Node corruption opponent: They can decode or fabricate communications using the secret key provided on the device or detector in addition to their skills as an external adversary. This is a complete takeover of the targeted node. HSP's main anti-corruption rival is as an outsider opponent, they have the ability to steal and modify the HSP's database.

4. RESULTS AND DISCUSSION

There is no correlation between session keys in our proposed approach, and new session keys were not derived from prior session keys. Randomly generated session keys are assigned to each user. N and HSP's previous and future sessions are unaffected by a single critical compromise. Both techniques need parties to validate the associated session key in real time before continuing conversation. Only incorporated parties have access to the master secret keys, which are used to encrypt and decode the session key. As a result, the approach under consideration allows for private communication. Our research has shown that even if a session key is compromised for whatever circumstance, the confidentiality of other previous and prospective sessions is not impacted.

These credentials are chosen separately from each other. There is no risk to the security of the master secret keys if a session key is leaked. Even if a session key is exposed, forward or backward security is maintained. To protect the node's tamper-proof smart card, just the master secret key is kept secret in our methods. All node owner secret keys are secured using the public key of the HSP. The only item that is kept secret is the HSP's private key. Cyber-thieves can utilise their master secret key kN to impersonate another user if they know the HSP's IP address and the device or smart card they are using is theirs.

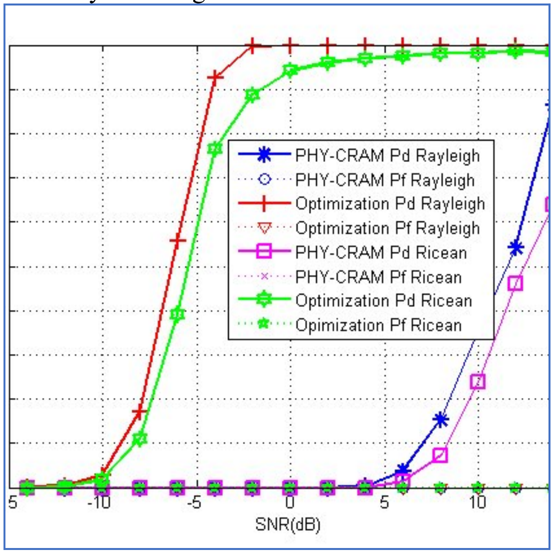

Figure 3: Performance comparison of authentication algorithm

Our approach can resist attacks resulting from the theft of a mobile user's device with very modest modifications. However, in order to avoid drawing the reader's attention away from the procedure, we failed to explain this. This problem can be solved in a variety of ways. Using the smart card's PIN (personal identification number) correctly is one approach. Without the right PIN, a cyberthief has no purpose for a stolen gadget. In a replay attack, an adversary tries to deceive one party by utilising a prior transmission from a different party as in the Figure 3.

Each session's communications should be checked for freshness, and timestamp and random number algorithms are two of the primary methods for preventing replay attacks. There are two procedures in our approach that ensure that the communication messages in each session are never reused, so that replay attacks may be avoided in any protocol. In order to deceive other participants in a user authentication system, an attacker would like to pretend to be one of the participants in the scheme as in the Figure 4. As a result, the adversary will be unable to get any relevant information from the public channel or pose as a legitimate party unless they have access to the secret key utilised by each of our protocols.

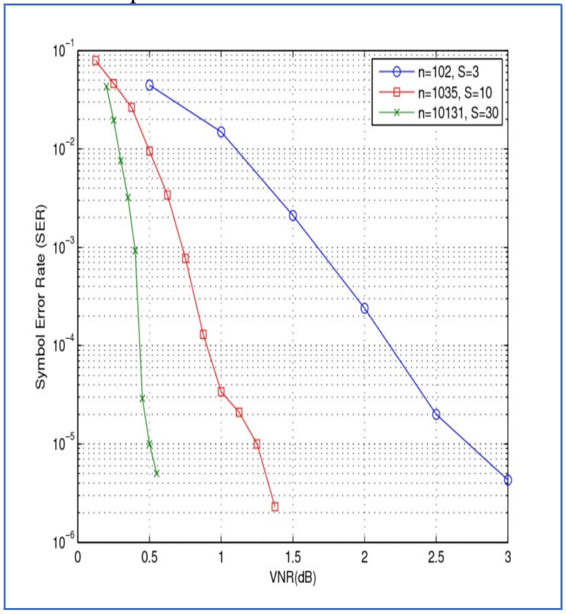

Figure 4: Error rate analysis

Latency, transmission power, dependability, and reserved bandwidth are all parts of QoS. Because of this trade-off, a proper balance must be found for each application depending on power consumption and dependability needs. The quality of service (QoS) issue is critical in WBAN, despite the fact that numerous solutions for WSN already exist. However, because to the disparate nature of WBAN's sensors, these solutions cannot be directly deployed as in the Figure 5. Resources restrictions, unexpected traffic conditions, networking destabilization, network instability, energy balancing, data redundancy, varied traffic kinds, packet criticality, and many sinks are just a few of the major issues in supporting QoS in the WBAN.

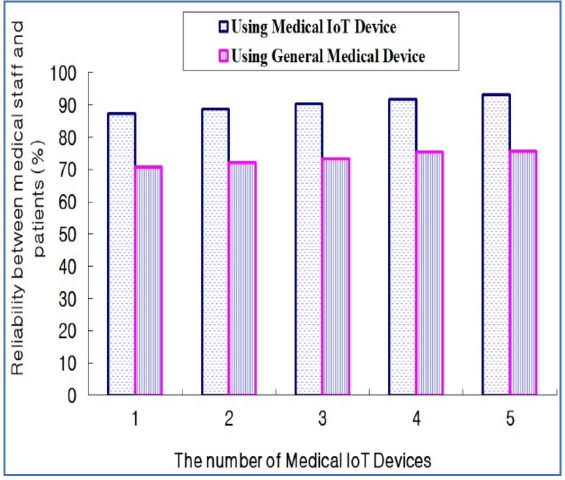

Figure 5: Reliability analysis

There are many others as well. Channel fading occurs as the node moves away from the gateway in WBAN because of the subject's motion. Insertion loss along and within the human body can also result in channel fading. Efficiency in perspective of bit error rate degrades due to this (BER). Using narrowband radio waves, or UWB, is being researched by a large number of researchers. The presence of water and flesh in the signal channel caused significant path losses, according to all measurements. The higher the frequency, the greater the path loss. Detached and remote sensor charging is frequently highlighted as a major impediment to their widespread adoption. Individual nodes requiring an external power source lose many of the benefits of wireless sensor networking.

Electronic circuits may now run longer on a given power source because to ongoing improvements in power management. However, this strategy has significant drawbacks when it comes to power harvesting/scavenging. Wireless sensor nodes can be powered by a variety of low-grade ambient energy sources, such as atmospheric disturbances, manpower, temperature sources, solar, and wind energy, and then transformed into usable electric energy through the process of energy harvesting. Low-power wireless electronics devices can benefit from energy harvesting devices as a battery alternative. thermoelectric generating is another kind of energy collecting that we found extremely fascinating.

Engineers have created a thermoelectric micro-generator with a new construction, in which the passage of heat via parts with varied thermal resistances causes local temperature changes in the device. The database system's ability to maintain data integrity is critical. Consistent data throughout its life cycle is called data integrity. Physicians' opinions are based on data from the database. The remote station must thus verify the data's integrity before releasing it to the doctors or preserving it in the patient's medical record. CRC checks and packet headers can be used to ensure the integrity of the data being transmitted.

E-Health systems employ databases for medical records, treatment guidance, drug and procedure efficacy evaluations, cost estimations, and improvements to medical facilities; these are only some of the uses of databases in e-Health. On the one hand, remote monitoring improves quality of life and healthcare, but on the other hand, it raises concerns about security and privacy. As soon as the information is posted on the internet, it is vulnerable to intrusion by hackers and other hostile actors. One of the most difficult aspects of establishing Electronic Health Records in an e-Health setting is ensuring the data's integrity, accessibility, and preservation. Authentication, security, and accessibility are among the most important elements of database storage and administration approaches.

5. CONCLUSION

The multiple levels of a mHealth system have been suggested in this work using an anonymous authentication technique. Health service providers (HSPs) medical servers can be authenticated using anonymous authentication nodes while mobile users can be authenticated using the second-tier controller nodes, and wearable body sensors can be authenticated using first tier controller nodes, according to this proposed system. To achieve a better balance between security, efficiency, and usability, we factored in the varying resource restrictions of the various nodes throughout the mHealth system. Through a combination of comprehensive assessments and conversations of security aspects, prospective attacks, and solutions we examine the security of our proposed method. Furthermore, our suggested system is tested and compared to other similar schemes, and the results are presented in a clear and concise manner. We demonstrated that our method surpasses the competition and offers a broader range of integrated and comprehensive anonymous authentication services than any of the alternatives. Using the Scope animator and the Systematic Evaluation of Internet Security Mechanisms and Services programme, we also tested our system's security, and the findings indicated that it meets all of the stipulated privacy and authentication criteria.

REFERENCES:

[1]. Akkaya, K., Younis, M., & Youssef, M. (2005). Efficient aggregation of delay-constrained data in wireless sensor networks. In Proceedings of the ACS/IEEE 2005 international conference on computer systems and applications, pp. 904–909. IEEE Computer Society.

[2]. Bao, S.-D., & Zhang, Y.-T. (2006). A design proposal of security architecture for medical body sensor networks. In International workshop on wearable and implantable body sensor networks (BSN'06), pp. 4–pp. IEEE.

[3]. Curtis D., Shih, E., Waterman J., Guttag J., Bailey, J. et al. Physiological signal monitoring in the waiting areas of an emergency room. In: Proceedings of BodyNets2008. Tempe, Arizona, USA, 2008.

[4]. Fu, Z., Sun, X., Liu, Q., ZHOU, L., & SHU, J. (2015). Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Transactions on Communications, 98(1), 190–200.

[5]. Kadayif, I., Kandemir, M., 'Tuning in-sensor data filtering to reduce energy consumption in wireless sensors networks' proceedings design automation and test in Europe Conference and Exhibition, 2004.

[6]. Kirbaş I., HealthFace: A web-based remote monitoring interface for medical healthcare systems based on wireless body area sensor network, vol. doi:10.3906/elk-1011-934., 2010.

[7]. Lai, D., Begg, R. K., and Palaniswami, M., eds, Healthcare Sensor Networks: Challenges towards practical implementation, ISBN 978-1-4398-2181-7, 2011.

[8]. Lee, H., Park, K., Lee, B., Choi, J., and Elmasri, R., "Issues in data fusion for healthcare monitoring," in Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments, 2008, pp. 3.

[9]. Medjahed, H., Istrate, D., Boudy, J., Baldinger, J., and Dorizzi, B., "A pervasive multi-sensor data fusion for smart home healthcare monitoring," in Fuzzy Systems (FUZZ), 2011 IEEE International Conference on, 2011, pp. 1466–1473.

[10]. Rameshkumar, C., and T. Ganeshkumar. "A Novel of Survey: In Healthcare System for Wireless Body-Area Network." In Applications of Computational Methods in Manufacturing and Product Design, pp. 591-609. Springer, Singapore, 2022.

[11]. Qutub Ali, B., Pissinou, N., and Makki, K., Approximate replication of data Using Adaptive filter in Wireless Sensor Networks, International symposium on Wireless Pervasive Computing, May 2008.

[12]. Kumar, Ramesh, and Rajeswari Mukesh. "State of the art: Security in wireless body area networks." International Journal of Computer Science & Engineering Technology (IJCSET) 4, no. 05 (2013): 622-630.

[13]. Zhen, B., Patel, M., Lee, S. H., Won, E. T., and Astrin, A., "TG6 Technical Requirements Document (TRD)", IEEE P802.15-08- 0644-05-0006.

[14]. 1. C. Ramesh Kumar, T. Ganesh Kumar, A. Hemlathadhevi, D. R. Thirupurasundari, "An Energy Efficiency Based Secure Data Transmission in WBSN Using Novel Id-Based Group Signature Model and SECC Technique," Journal of Internet Technology, vol. 24, no. 3 , pp. 683-696, May. 2023.

[15]. Rameshkumar, C., and A. Hemlathadhevi. "Automatic Edge Detection and Growth Prediction of Pleural Effusion Using Raster Scan Algorithm." In Proceedings of International Conference on Computational Intelligence and Data Engineering: Proceedings of ICCIDE 2018, pp. 77-87. Springer Singapore, 2019.