Schemes for Secure Key Agreement and Authentication in Wireless Body Area Networks

J.Harirajkumar[1], R.Thandaiah Prabu[2], S.Diwakaran[3], Shamitha.C[4], Anitha G[5]

[1]Associate Professor, Department of Electronics and Instrumentation, Sona College of Technology, Salem.

[2,5]Associate Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai.

[3]Associate Professor, Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Srivilliputhur.

[4]Assistant Professor, Department of ECE, Manipal Institute of Technology, MAHE, Bengaluru Campus,Bengaluru.

[1]harirajkumar.j@sonatech.ac.in, [2]thandaiah@gmail.com, [3]s.divakaran@klu.ac.in, [4]shamithac2@gmail.com, [5]anipsg09@gmail.com

Abstract.

In recent years, technological breakthroughs in wireless communication as well as systems engineering, electronic components, fitness bands, and nano-materials have resulted in the development of a new approach in Internet of Things (IoT)-based system that focuses known as Wireless Body Area Networks (WBANs). Wireless Body Area Network (WBAN) is a fascinating sector that, if used in the procedure of health records surveillance, has the potential to enhance the overall standard of living. Nevertheless, the portability and public source provided by wireless connections have led to a series of security flaws, which might also end in the compromising of sensitive wellness data concerns. Consequently, there was a requirement for the development of a method to respect and protect wellness information from all types of security breaches. In recent years, a trust management system has been presented, which is predicated on the premise that perhaps the foundation node is trustworthy. Despite this, it does not appear to be practicable in practice. The authors therefore present a minimal encryption method that is composed of three layers of security and provides anonymized key exchange protocol and verification for information sent via a wireless network. When tested against different known computer hackers, including the ground station penetration assault and sensor networks account hijacking; the authenticated key agreement technique demonstrates its effectiveness in protecting against them. The system was officially confirmed using BAN logic and unofficially modeled to use the Automatic Verification of Internet Safety Protocols and Apps (AVISPA) tool, both of which were used to verify the system. The suggested secret negotiation and system is to ensure was further evaluated in light of the findings of other comparable studies, which were also considered. The simulation outcomes and detection techniques show that the suggested enhanced scheme has addressed the many shortcomings that have been found in terms of memory needs, computing expenses, and verbal exchange costs, among other things.

Keywords. Patients' medical surveillance; verification; WBAN; connectivity; cyber threats.

1. INTRODUCTION

Because of advancements in circuits and gear arrangement, the length of biomaterials has been decreased to the point that they can now be worn on clothes or the organism, or perhaps even inserted within the body, without compromising performance. Wearable health devices are expected to see a significant increase in their use worldwide as a result of continued expansion in the planet's population, trying to improve average lifespan, rising chronic illnesses, expanding use of bio-sensors throughout sporting events, and increasing prevalence of medical equipment in physical training [1] [26]. With the digital revolution, particularly the sensing connection, the possibility of health monitoring has been made feasible, allowing for an improvement in the standard of living. With the assistance of this omnipresent equipment, the health of the individuals can now be tracked in real time, something that has never been possible before. As a result of the WBANs, individuals have more freedom to go about their everyday lives while knowing that their healthcare is being adequately looked after by a highly trained medical professional.

Because of its promising future in a wide variety of uses, WSN is attracting increasing attention from both academic and commercial. In its most basic form, WSNs are intended to distribute a group of wearable sensors across an isolated region, gather and communicate environmental information to a base or distant location, and then to gather and communicate further environmental information. The raw information is then analyzed online or in person in accordance with the technical specifications before being sent to a distant server for a full evaluation [2] [19] [25]. When a sufferer is outside of the hospital, patients to access may be very valuable to physicians. Wearable medical sensor networks (WMSNs) are at the heart of this concept, and their deployment is critical to realizing the full promise of this innovation. Wireless Medical Sensor Networks (WMSN) in application areas have made significant contributions to the advancement of the healthcare business in the twenty-first century [3][4] [23] [24]. Wireless sensor networks (WSNs) in multiple health sectors are expanding at an extraordinary speed in both advanced and emerging nations in order to deliver a high level of treatment to patients. The devices then collect biomedical signals from the individuals, including such cardiac rates, beats, warmth, and so on, via the use of wireless technology. Healthcare personnel may access global surveillance in real time using portable devices, which they can carry with them. In this regard, wireless sensing technology may provide important instruments for the surveillance of the wellbeing of the individual and the medical management on a continuing basis. As a result, ongoing study into wireless sensor networks is an attractive and rapidly expanding field of medicine. There are several entities that make up the Internet of Medical Things

(IoMT), including treatment centres, state hospitals, hospital instruments, and consumers of e-health. In a Wireless Body Area Network (WBAN), clusters and cores of sensor systems that operate in, on or around a person and serve a variety of health and non-medical purposes are connected [4] [20]. As a result, in an old-world scenario, the development of universal care would include constant health monitoring and the least amount of effective interaction among client and therapist. Users and the gateway both typically have a large amount of storage and processing capacity, but sensors may vary over time. A sensor is equipped with restricted resources, such as a small amount of memory and a small amount of battery power. Because of this, it is vital to make efficient use of the sensors. When someone illegally obtains patient information, the patient's right to privacy is violated. If a patient's data is compromised, medical practitioners may make an inaccurate diagnosis, which might have life-threatening repercussions. A encrypted communication infrastructure is consequently required in order for business to thrive. Unpatched vulnerabilities such as weak cryptographic techniques [5] have been investigated, and these include verification, data transmission verification, inactive credential sensing, key impersonating, as well as attacker capabilities, among others. As distributed systems become more widely deployed, multi-server settings will become more safe and resilient in their provision of communication networks [6].

In order to monitor physical aspects such as vital signs, hypertension (BP), warmth, Electrocardiography (ECG), as well as other parameters, portable or implanted equipment are placed to the body of the patient and communicate with one another using wireless technology [22]. As a result, WBAN offers a comprehensive evaluation system for individuals that are both convenient and effective. The usual design for WBAN is shown in Fig. 1, which consists of collecting information from sensors and delivering it to a patient database over communication networks, where a specialist doctor may readily see patient data in order to evaluate and treat as needed.

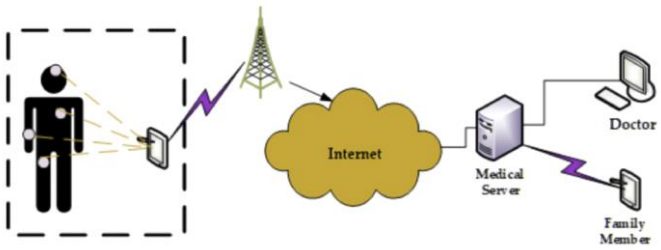

Figure 1: The WBAN's characteristic architectural style.

In the publications, it has been discovered that there are numerous different types of authentication mechanisms available; a report written by Rehman et al. divides the security mechanisms into 4 segments, which are biological, data encryption-based, proximity-based, and communication-based [7]. Other categories, but at the other hand, may be found in the literature [8, 9]. Identifies the central identification techniques rely on the physical characteristics of patients to establish trust [10] [21] [27]. WBAN devices with limited resources may benefit from these strategies to a sufficient degree. However, a significant disadvantage is their susceptibility to denial-of-service (DoS) assaults, and it is hard to assess biomedical parameters that are similar across all devices on different portions of the person's body.

The chances of achieving the desired verification systems offer reliable verification when used in conjunction with a key establishment, but they need additional storage and are computationally demanding. Nevertheless, as compared to typical asymmetric methods, Elliptic Curve Cryptography (ECC)-based techniques spend less computational power, while featherweight systems spend far less computational power when linked to ECC-based techniques.

The most significant aspect of this research is to close the security vulnerabilities highlighted by Kompara et al. [11] by altering their method to address the issues that were discovered, which are as follows:-

- On the basis of hashing and XOR algorithms, we have presented an improved key negotiation and best strategy for use in distributed systems. Adding new features to existing encryption techniques, the proposed technique goes beyond the security characteristics provided by the initial condition and incorporates new ones such as defence against Intermediate Node (IN) penetration, data transmission impersonator, and central node mutually acceptable threats on top of the existing encryption techniques.
- We have formalized our system by using BAN reasoning, and that we have informalized it by utilizing one of the most well-known tools specifically developed for this reason, known as AVISPA.
- When related to competitor identification systems, the suggested access control has lower memory and transmission costs, resulting in superior efficiency.

The remainder of the article is arranged as follows: Chapter 2 describes a problem definition, Section 3 portrays a prototype system as well as an implacable enemy prototype, Section 4 gives the proposed technique, Section 5 indicates the typical program's vulnerability scanning, including encryption techniques, authoritative and unofficial assessment, Section 6 portrays the achievement study to compare of our arrangement with result of these findings, Section 7 portrays conversation on our arrangement, and Section 8 contains an inference and recommendations for further research.

2. Related Study

The Internet of Things (IoT) offers tremendous promise in the field of social and healthcare technologies. Some Internet of Things (IoT) information in this report, including such body region monitors, enhanced medical systems, monitoring devices, mobile internet platforms, collection and presentation of medical studies, and so on, are particularly interesting. The method [12] was shown to be subject to damage on the client, destruction of keys offsite, and temporary assault on discussion important information by Shuai et al. in 2019 [13]. The suggested technique makes use of improved elliptical encryption and is safe enough to protect consumers from pattern remembering assaults as well as attacks on lost or damaged contactless payment

verifiers. This framework was established by the author in order to prohibit the transmission of information to outsiders. In order to facilitate communication with computations and settings, the method is accurate, simple, and simple. In order to verify the suggested structure, comprehensive detection accuracy was carried out with the help of the AVISPA tool.

An Elliptic Curve (ECC) based three-factor wireless communication sensor identification technique was created by Li et al. (2019) [14], which used error checking algorithm and fluency engagement strategies to handle biometric information and secrecy moving forward. Besides using the flexible checkers and nectar list approaches to tackle the issue of regional credential lookup, while fighting assaults on portable devices, the mushy inspector and nectar listing approaches were also used. Even though Li et al. employed the fuzzy checker approach and asserted that their remote medical monitoring internet layer [14] fulfilled various safety requirements, we discovered that it was not able to survive repeated replay assaults.

In 2019, Shuai et al. [13] developed a three-factor authentication process that is both inexpensive and efficient for controller of On-Body Wireless Networks (OBWN) clients, which they deployed in 2019. The suggested approach makes use of a special hashing chained system in order to ensure prospective users' privacy, as well as a fictitious identification is provided to prevent synchronization attacks from being launched. The suggested framework uses a pseudonym identification strategy to ensure user anonymity while also providing the possibility of secrecy via the use of an one-time hashing chain mechanism. The researchers [15] have demonstrated that their technique [13] still suffers from three security flaws: download vocabulary depreciation assaults, empowered cyberattacks, and password recovery problems.

It is necessary for significant quality to have enough of capacity, dependable and functional network technologies and power processes as well as high-quality service support (QoS). Inter environments are used by caregivers to guarantee that smooth solutions are supplied to finish. Health clinical devices sense a large amount of data that must be transferred through servers, which is difficult in a single component. By enabling a multi-server system, hospitals healthcare devices can create a large amount of data that must be communicated via servers. Because the information being transferred is sensitive, it is crucial to evaluate safe online interaction while ensuring data security. The opponent may attempt to disrupt the delivery and either discard or change the narrative as a result of this. In order to safeguard the information, several studies have introduced security mechanism; however these schemes are subject to certain assaults among other things. In such a successful transformation in a dispersed client, nevertheless, the lack of an identification technique that allows multi-server privacy is still a concern. According to article [16], an authenticating users technique for a multi-server context is developed, which makes use of wearable medical sensing devices (Cross-SN). The technique is accomplished via the use of a smart card, a password, and unique user identification. The suggested technique makes use of cryptographic algorithms, as well as Burrows–Abadi–Needham (BAN) logic, to guarantee authentication mechanism and assess the stability of the model. It provides appropriate security against responses, impersonator, and powerful malicious activities, as well as encrypted connection in multi-server entities that connect with one another. It is free to use.

3. METHODOLOGY

Authentication mechanism formation is performed in a minimal manner using the signature scheme proposed by Komapara et al. [1]. Figure 2 depicts a three-tiered network model of their design, which is representative of their approach. In their architecture, layer 1 featured a sensor node designated by the letter N, which acquired data but was limited in terms of resources. The Intermediary Node (IN) is often a smartphone, which is referred to as tier 2. Information from sensor network (N) is received at this tier and sent to layer 3, which is the Hubs network (HN). In many cases, helicopter nurseries (HNs) are large medical servers with a lot of resources, and their job is to provide secure and convenient universal health care services to the community.

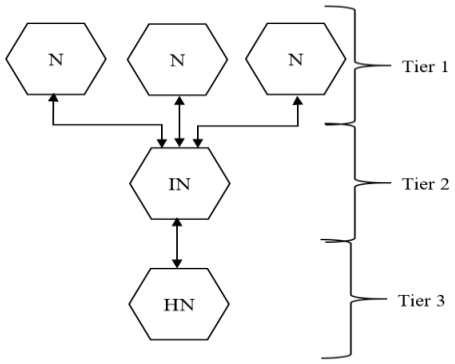

Figure 2:Modeling of the Kompara et al. system using networks

This technique is divided into three parts: startup, enrollment, and verification. Initializing is the first step. Setting and registrations are carried out by the job System Administrator (SA) under the premise that now the route is protected, whereas the verification stage is carried out from the role Head of Network (HN) under the premise that now the route is accessible. The researchers have made the assumption that the encrypted channel is accessible for SA in order to communicate information among N and UN. When it comes to the authentication step, though, this presumption is not made, and as a result, the attacker may be able to participate. A mutual key is used to create a secure interface between N and HN, and it is the duty of HN to expedite the transaction of verification and consensus on a similar key.

a. ANALYSIS OF KOMPARA'S SCHEME

Following a thorough examination of Kompara et al. [11]'s system, the following three forms of assaults were identified as being under research in their model:

Using the example of Figure 2, the job of IN in the aforementioned strategy is to convey all response message to HN while also saving tuple. It should also be noted which neither IN nor IN itself is validated by HN, despite the fact that both are used to verify N. As a result, it may become a weakness that can be exploited to launch an IN takeover attempt. As collaboration is the primary function of IN, giving up IN would result not just in disrupting the entire teamwork but also making it possible for an opponent to retrieve individuality in order to commence some other consecutive target in order to make concessions the network device as a result of the negotiated settlement of IN. When IN is either a wristwatch or a smartphone, the likelihood of it being stolen is great. As a result, the likelihood of IN remaining uninsured is extremely small in these kind of situations.

It has been pointed out by the creators of the previously described system that if IN is penetrated, which is a possibility, the variables id_N and x_N may be divulged, resulting in sensor node spoofing attacks, as previously indicated. After successfully seizing the node and collecting the correct parameters as previously indicated, an attacker may become a member of the verification phase by impersonating the node using HN.

Therefore, the technique is predicated only on the assumption that HN is safe, that is untenable in a pragmatic way due to the possibility that HN will be compromised if the method is used. Despite the fact that it is nearly impossible for any opponent to generate a valid integer (β,η,μ), this will only be possible if the opponent has access to the central controller (which is not the case) (HN). As a result, penetrating the HN could disclose all of the knowledge, including the combination lock, which is symbolised by the letter k_{HN} on the computer.

In this section, we will explain the network approach and the competitor model of our suggested method.

b. NETWORK MODEL

In our approach, we had preserved the three-level network topology presented in [11], although the connection among N and IN is somewhat distinct from the connection among N and HN. Because it does not save any information about the connection between N and HN, the IN operates as a relaying node, giving it less influence over the interaction between the different networks. A N-IN communication is done when information through one or even more Ns is now to be transmitted to a destination other than HN. Consequently, the IN plays a supporting function in the overall communication by collecting information from sensors and relaying it to the HN. Figure 3 depicts a network model of the Internet.

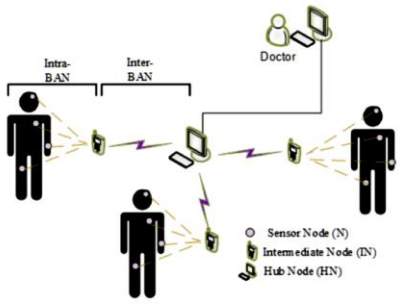

Figure 3: Our technique is based on a network concept.

c. RIVAL MODEL

We made the assumption that an enemy could carry out the following:

- The HN is regarded as reliable, as well as an attacker might not have been able to recover the key code k_{HN} if the HN is compromised.
- The attacker may be able to decrypt the proper communication route and fraudulently introduce data, as well as change or replay previously sent material;
- An intruder may get access to the encrypted keys by corrupting the N, with the goal of interfering with reciprocal established connection. Furthermore, because of financial constraints, N also isn't actually safeguarded.
- When we exercise a well based on the dynamics for our technique, we presume that individuals conversing are using insecure communication routes.

4. SECURITY ANALYSIS OF SUGGESTED METHODS

This chapter consists of three sections. First, we will describe the security mechanisms that the suggested scheme provides in order to protect against additional internet. After that, we discuss casual testing of the present scheme that use the AVISPA tools as well as, finally, we discuss comprehensive security validation of the suggested method utilizing BAN logic.

A. SECURITY FEATURES

It is in this section that we describe the robustness of our system against the assaults indicated above, in addition to the assaults described below:

Replay attack is the most straightforward kind of assault, and our technique is secured against it by introducing a timing t_N at the beginning of the verification step. The date is inserted in such a manner that it could be changed by the attacker. If a communication is repeated after just a period of time, the alteration will be obvious, as well as the communication will indeed be refused as such. It is also necessary to use a randomized nonce r_N when repeating the information since the nonce varies with each request. As a result, it is not feasible to launch a replay assault.

1) SENSOR NODE IMPERSONATION ATTACK

The suggested approach offers security against such a sort of attack since the opponent has no means of knowing the descriptive values of $Z_N;x_N$ that are necessary to build a valid tuple that can be used to progress more with the verification process after the first authentication step.

2) TRACKING AND ANONYMITY ATTACK

Due to the fact that now the network IN is just operating as a relaying that passes communications without saving data, a monitoring assault is not feasible due to the fact that no data can be generated via IN. A consistent thing is used for the calculation of tid_N, that's just transient and would be modified within every transaction for node N to UN. This means that this variable was picked at randomness and could be predicted by an opponent. As a result, our strategy is resistant to these threats.

3) BASE STATION CAPTURE ATTACK

The opponent might acquire the HN by using the HN hijacked information assault and in this scenario; the opponent would also be able to grab the universal key K_{UN} in our system. Other crucial factors, such as $x_N^+, \beta, \eta, \mu, k_s$, cannot be constructed since the universal key K_{UN} has been modified by the Xor operation, which has added a new random vector e_N. As a result, the opponent has no means of knowing since information is not made publicly available. As a result, our strategy is likewise resistant to this assault.

4) FORWARD/BACKWARD SECRECY

It is impossible for a malicious opponent to infer the former key pair and the following authentication protocol if he forges key exchange k_S. This is due to the fact that k_S is generated using variables and x_N^+, which are in turn dependent on the hashing algorithm and a complete new randomized value, respectively. Furthermore, having k_S does not provide information on both of these characteristics. As a result, this strategy is effective against this assault.

B. INFORMAL PROOF USING AVISPA

AVISPA is a tool that evaluates the security of our system and we give it here as an example of casual validation using this instrument. AVISPA's High-Level Protocol Specification Language (HLPSL) has been used to design the standard, which was then tested in the field. HLPSL style is converted into Intermediate Format (IF), that is then processed by back end inspection methods such as On the-Fly Model Check (OFMC) and Constraint Logic-based Attack Searcher (CLAS) (CL-AtSe). Such approaches provide evidence about whether a strategy is secure or otherwise, and if it can withstand proactive and reactive assaults.

Several HLPSL roles, including the administrator (SA), sensornode, and hub node, are used to perform the startup, enrollment, and verification processes. By utilizing the ecosystem role, it is possible to describe invader information, worldwide limits, and the scheduling with one or even more encounters. The following are brief explanations of the various roles:

1) ROLE SYSADMIN

The SA is aware of most other agencies, the key generation, hidden keys such as KUN and KN, as well as the identification of N, which is the IDN. The startup and certification steps of our identification strategy are carried out by this role. In this example, the elements XN, AN, and ZN are defined as memory locations, as well as the contents of these factors are determined to use the Hash function. These data are subsequently sent to N using a secure channel.

2) ROLE SENSORNODE

This job is responsible for carrying out the duties carried out by N during the verification stage of our system. Sensornode (N in our system) is analogous to the administrator job in that it is aware of all clients, the asymmetric key, have sent routes, instance variables, hashing algorithms, and protocol IDs. On the communication page, it gets the signal supplied by SA through the security gateway and executes the operations defined in the suggested verification stage, after which it lets people know back. Not to note that it is among the most significant positions that is directly involved inside the verification process that deserves to be mentioned here.

3) ROLE HUBNODE

It is yet another crucial function that the United Nations plays, and it takes an active position in the verification process. It is identical to its previous roles in that it understands all clients, the symmetrical key, its private keys, instance variables, hashing algorithms, protocols IDs, and the send/receive channels, among other things. It received a response from N and decrypt the data it with the help of a symmetric cryptography he created. It uses the public channel to carry out the remainder of the functions that were described during the authentication step. The secret key is then calculated at the conclusion of the programme.

4) ROLE SESSION

All of the agencies and roles that were discussed before are invoked in this HLPSL code. Aside from that, basic fixed elements are identified, and the have just sent routes for SA, N, and HN are denoted as SSAch, RSAch, SNch, RNch, SHNH, and RHNch, accordingly, in the following tables.

5. RESULTS AND DISCUSSIONS

Here we examine the energy usage, storage, computing, and transmission losses of our strategy in order to assess its effectiveness. The fact that we make this comparability with a state-of-the-art verification system possible since they are connected to one another and many of them are an improvement over previous work, as mentioned in Section I, is worth emphasizing here. As a result of this analysis, the effectiveness of the suggested authentication technique is also highlighted. The security characteristics comparison in Table 1 further demonstrates that our system meets all of the security criteria on which we place particular emphasis.

	[17]	[18]	Ours
Z1	Y	N	Y
Z2	Y	Y	Y
Z3	Y	Y	Y
Z4	N	Y	Y

Z5	Y	Y	Y
Z6	N	Y	Y
Z7	Y	Y	Y
Z8	Y	Y	Y
Z1: IN compromise attack, Z2: Replay attack, Z3: Sensor node impersonation attack, Z4: Hub node spoofing attack, Z5: Tracking and anonymity attack, Z6: Base-station capture attack, Z7: Forward/backward secrecy attack, Z8: Man-in-the-middle attack			

Table 1: Comparing safeguards to peer research is a good idea.

According to our design, the N contains the tuple (id_N;x_N; a_N; Z_N) as well as the key exchange k_S. Because IN is our scenario doesn't really retain anything value, but rather merely serves as a relay node, there is no need for any memory. The UN holds variables such as K_{UN};id_N;K_N as well as the key agreement k_S, which are each 160 bits in length. Kompara et alapproach's saved four values on HN that were connected to N, but only three variables are kept on the UN in our scheme. As a result, our method requires less storage space in this aspect. We will assume that N contains parameters with $|id_N|=|x_N|=|a_N|=|Z_N|=|K_{UN}|=160$ bits every, as shown in the table. On the next page, you will find a review of the installation costs amongst peer systems.

	N	IN	UN(HN)
[17]	800b	0b	160b
[18]	640b	640b	(320+160n)b
Ours	800b	0b	(480n+160)b
n: No. of sensor nodes, m: No. of the intermediate node, b: bus			

Table 2: Storage costs are compared to the cost of peer work.

As shown in our diagram, the sensor node (N) delivers the tuple (tid_N, a_N, b_N,t_N) to the intermediate nodes (HN) via IN, which just relays the information to the receiver without changing something to it. Assuming that $|t_N|$ is equal to 32 bits, the connection cost N ∏UN is 3(160) + 32 = 512 bits, and the transmission cost UN∏Nis 3(160) = 480 bits. Table 4 displays a comparison of our strategy with that of our competitors.

Peers	N ∏ IN	IN ∏HN	HN ∏ IN	IN ∏ N
[17]	672	672	640	640
[18]	672	1344	960	480
Ours	512	512	480	480

Table 3: When compared to peer work, the communication overhead is lower.

The variables t_{xor} and t_h should be used to reflect the long it takes to perform one XOR algorithms and one Hashing. As part of the authentication step, N conducts six XOR actions and three hashing algorithms, totaling nine in our approach. Assuming that the XOR action requires little computing, the actual calculation is that of the hashing algorithm; as a result, it is denoted as $3t_h+6t_{xor}\approx3t_h$in the representation. In a complete scheme, a total of 10 XOR actions and 6 cryptographic algorithms are done, which is denoted by the notation $6t_h+ 10t_{xor}\approx6t_h$.

Because our hashing is almost equal to Komapara's approach (apart from a little increase in the hashing), the computational cost and power efficiency are identical to those of Komapara's method. A 32-bit Cortex-M3 microprocessor operating at 72 Megahertz, that was also used by Kompara et al. and Li et al., requires 0.06 ms, but an XOR controlling operation takes too little time to complete, according to the authors (see Figure 1). This results in a hashing algorithm taking 0.18 milliseconds for N and 0.36 milliseconds for UN to complete. With regard to peers in the field, Table 4 provides a comparative analysis of processing costs and timelines in relation to competitors.

In this part, we make it easier to compare our plan with other schemes by providing a table of comparisons. Because no data is saved on our scheme, the available storage cost is lower than the installation costs of the majority of the plans evaluated in Table 2, with the exception of the system that has a memory usage that is equivalent to our scheme. Additionally, while comparing the costs of transmission, it has been shown that our plan incurs a fairly modest amount of money. When comparing our scheme to other procedures, it is also apparent from Table 4 that our method accrues no additional cost when delivering a

message from IN to UN, and we have reduced the good communication price between IN - HN and conversely, as seen in Figure 4. So it is both economical and inexpensive in this sense, making it an excellent choice. Furthermore, it is worthwhile to emphasize that now the transmission price for our method is the cost of sending information between N to UN (in our example) and conversely.

Additionally, the computational overhead and calculation time for our system, as given in Table 4, have been determined by comparison to those of other methods. It is also clear that our method incurs a tiny increase in processing cost and time when compared to Kompara et al. [11], but we consider this to be a small price to pay for an improved and efficient approach. The United Nations is a generally formidable organization that can readily handle this task. Furthermore, Table 6 displays the specifics of our program's energy usage and compares it to those of others.

Peers	N (mJ)	HN (mJ)
[17]	0.021	0.036
[18]	0.036	0.048
Ours	0.021	0.043

Table 4: Examining the energy use in relation to peer work

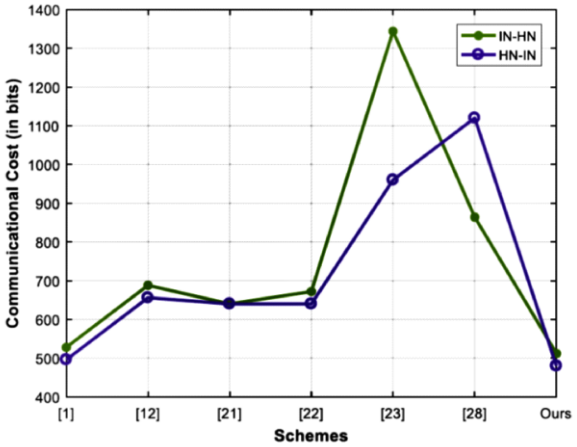

Figure 4: The expense of information in relation to peers.

In this study, we offer a novel anonymized, minimalist approach that is both simple and effective. We conducted an analysis of the Kompara et al. [11] system and identified a few security weaknesses in it. The first weakness is an IN compromises attempt, which is created by storing the identity id'_{IN} of IN throughout the established connection, which remains intact throughout the process. The adversary may estimate the identity of the victim and use that information to start the penetration assault. By not storing anything on IN and using it just as a reporting node, we are able to defend ourselves from this kind of assault. The second issue is data transmission impersonating, which is a result of the first assault and is a repercussion of it. The progressive and irreversible hash function was used to safeguard another secret integer, which has the identification id_N and is safeguarded by the progressive and irreversible hash function. The approach presented by Kompara et al. is reliant on the assumptions that HN is trustworthy and that the private key k_{HN} cannot be disclosed even if HN is leaked (as has been shown). Given that this assumption appears to be impractical in practice, they had provided a fix in our approach by updating the primary key to reflect this fact. This leads to a different password manager that is inaccessible to the adversary, unless the adversary gains access to the key management system via some other means (HN). Furthermore, we have maintained our emphasis on making our scheme as light as possible. As shown in Fig.13, the language and communication price of our system is much lesser than the price of the peers' plan. Because HN (in our case, UN) is often used as a service and has more demanding capabilities than N, which would be a resource constraint, we have kept the bulk of the operational weight on it. This has resulted in lower processing resource consumption for N than the similar values for HN, as seen in Figure 5.

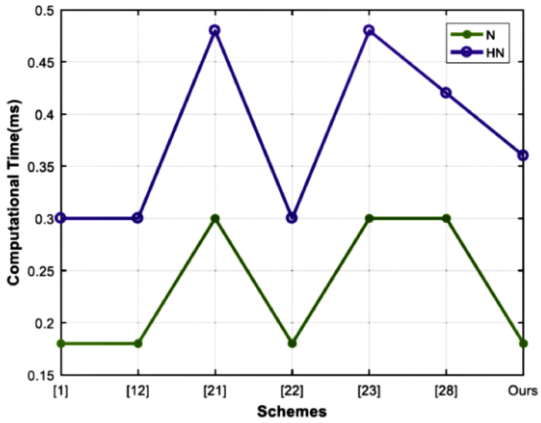

Figure 5: The cost of computing in contrast to other competitors.

6. CONCLUSION AND FUTURE SCOPE

Our major focus has been on reviewing the recently provided method by Kompara et al., as well as highlighting a few weaknesses such as data transmission deception, IN breach assault, and military radar takeover assault are all possibilities. We presented a technique to address these issues while maintaining the secrecy and inexpensive security mechanisms that was previously used. Furthermore, we have shown reciprocal authentication scheme negotiation of our system utilizing BAN reasoning, and we've also presented an unofficial assessment using the AVISPA program, which demonstrated that perhaps the new system is resistant to very well threats and may be used in a production environment. Also included is a calculation of the actual quality of our system in terms of data collection and transmission, processing, and power consumption. Lastly, we conducted a comparison of our approach with some of the most current relevant research. As a consequence of the simulated data and security assessments, it has been shown that the suggested digital certificates are not only resistant to a variety of common threats, but they are also economical and ultralight in storage capacity, connection, compute expenses, and duration.
A possible future step would be to combine this better authentication technique with physical measurements in order to reap the advantages of both technologies.

7. REFERENCES

[1]Shokeen S, Parkash D. A Systematic Review of Wireless Body Area Network. In: IEEE 2019 International Conference on Automation, Computational and Technology Management (ICACTM). 2019;p. 58–62.
[2] Yu, S.; Park, Y. SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless SensorNetworks. Sensors 2020, 20, 4143. [CrossRef] [PubMed]
[3]Gardaševi´c, G.; Katzis, K.; Baji´c, D.; Berbakov, L. Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare. Sensors 2020, 20, 3619. [CrossRef]
[4] Khalid, H.; Hashim, S.J.; Ahmad, S.M.; Hashim, F.; Chaudary, M.A. Cybersecurity in Industry 4.0 context: Background, issues,and future directions. Nine Pillars Technol. Ind. 2020, 263–307. [CrossRef]
[5] Ever, Y.K. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks.IEEE Syst. J. 2018, 13, 456–467. [CrossRef]
[6] Khalid, H.; Hashim, S.J.; Syed Ahmad, S.M.; Hashim, F.; Akmal Chaudhary, M. Security and Safety of Industrial Cyber-PhysicalSystem : Systematic Literature Review. Palarch'S J. Archaeol. Egypt/Egyptol. 2020, 17, 1592–1620.
[7] Z. U. Rehman, S. Altaf, and S. Iqbal, ``Survey of authentication schemes for health monitoring: A subset of cyber physical system," in Proc. 16th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST), Jan. 2019, pp. 653660.
[8] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, ``A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," Sustain. Cities Soc., vol. 50, Oct. 2019, Art. no. 101660.
[9] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, ``Authentication techniques and methodologies used in wireless body area networks," J. Syst. Archit., vol. 101, Dec. 2019, Art. no. 101655.
[10] H. Tan and I. Chung, ``Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," IEEE Access, vol. 7, pp. 151459151474, 2019.
[11] M. Kompara, S. H. Islam, and M. Hölbl, ``A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," Comput. Netw., vol. 148, pp. 196213, Jan. 2019.
[12] Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An enhanced three factor based authentication protocol using wirelessmedical sensor networks for healthcare monitoring. J. Ambient. Intell. Humaniz. Comput. 2018, 1–22. [CrossRef]
[13] Shuai, M.; Liu, B.; Yu, N.; Xiong, L. Lightweight and secure three-factor authentication scheme for remote patient monitoringusing on-body wireless networks. Secur. Commun. Netw. 2019, 2019. [CrossRef]
[14] Li, X.; Peng, J.; Obaidat, M.S.; Wu, F.; Khan, M.K.; Chen, C. A secure three-factor user authentication protocol with forwardsecrecy for wireless medical sensor network systems. IEEE Syst. J. 2019, 14, 39–50. [CrossRef]
[15] Mo, J.; Hu, Z.; Lin, Y. Cryptanalysis and Security Improvement of Two Authentication Schemes for Healthcare Systems UsingWireless Medical Sensor Networks. Secur. Commun. Netw. 2020, 2020. [CrossRef]
[16] Khalid, H.; Hashim, S.J.;Syed Ahmad, S.M.; Hashim, F.; Chaudhary, M.A. Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network. Electronics 2021, 10, 790. https://doi.org/10.3390/ electronics10070790

[17] C. Chen, B. Xiang, T. Wu, and K. Wang, ‘‘An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks,’’ MDPI, vol. 8, p. 1074, Dec. 2018.
[18] A. M. Koya and D. P. P., ‘‘Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network,’’ Comput. Netw., vol. 140, pp. 138–151, Jul. 2018.
[19] M. Tamilselvi, G. Ramkumar, G. Anitha, P. Nirmala and S. Ramesh, "A Novel Text Recognition Scheme using Classification Assisted Digital Image Processing Strategy," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-6, doi: 10.1109/ACCAI53970.2022.9752542.
[20] Ayyadurai, M., Ramkumar, G., &Anitha, G. (2021, June). Investigation on Tunable antenna with Polarization Using Cascaded BLC Feed Network. In *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 257-260). IEEE.
[21] G. Ramkumar and E. Logashanmugam (2016). “An Effectual Facial Expression Recognition Using Hmm” IEEE International Conference on Advanced Communication, Control & Computing Technologies in Syed Ammal Engineering College, Ramnathapuram
[22] G. Ramkumar, G. Anitha, P. Nirmala, S. Ramesh and M. Tamilselvi, "An Effective Copyright Management Principle using Intelligent Wavelet Transformation based Water marking Scheme," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-7, doi: 10.1109/ACCAI53970.2022.9752516.
[23] M. Benisha et al., "Design of Wearable Device for Child Safety," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 1076-1080, doi: 10.1109/ICICV50876.2021.9388592.
[24] Prabu RT, Benisha M, Bai VT. Characteristics of Alpha/Numeric Shape Microstrip Patch Antenna for Multiband Applications. InInternational Conference on Intelligent Systems Design and Applications 2018 Dec 6 (pp. 880-895). Springer, Cham.
[25] A. G, S. K. M, M. Ayyadurai, S. K. C and G. Ramkumar, "Design of Miniaturized Single Bit MEMS Phase Shifter using MEMS Switches," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 235-239, doi: 10.1109/ICOEI51242.2021.9453063.
[26] R, Thandaiah Prabu and M, Benisha and V, Thulasi Bai, Design of Wearable Antenna in Wireless Body Area Network (July 31, 2019). Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT) 2019, DOI: http://dx.doi.org/10.2139/ssrn.3429752.
[27] G. Ramkumar, P. Parkavi, K. Ramya and M. S. Priya, "A Survey On Sar Images Using Image Processing Techniques," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 1097-1100, doi: 10.1109/ICACCS48705.2020.9074261.