IoT Based on Wireless Area Body Networks

*Dr.Bibin A D[1], Mrs R Malarvizhi[2], Dr. Ben M. Jebin[3], Dr.Sam Abraham[4]

1 Assistant Professor, Department of Computer Science, Nadar Mahajana Sangam S Vellaichamy Nadar College, Madurai. E-**mail: bibinraj.ad@gmail.com, *Tel.: +91-7598515734***

2 Assistant Professor, Department of Computer Science, Nadar Mahajana Sangam S Vellaichamy Nadar College
Madurai. E**-mail: malarvizhi@nmssvnc.edu.in.**

3 Assistant Professor, Researc Department of Computer Science, Malankara Catholic College, Mariagiri,
E-mail: **benmjebin@gmail.com, Tel.: +91-9443391050**.

4 Assistant Professor, Department of Computer Applications, Malankara Catholic College, Mariagiri,
E-mail: **samabraham123@gmail.com, Tel.: +91-8848589501**.

(Affiliated to Madurai Kamaraj University, Madurai)

**Corresponding Author* E-mail: bibinraj.ad@gmail.com, *Tel.: +91-7598515734*

ABSTRACT

Internet of Things (IoT)-based wireless body area networks (WBANs) play a key role in modern medical systems for monitoring patient health. WBAN has the ability to collect real-time biological information from the patient's body through specific intelligent sensors and transmit the collected information to remote doctors and medical professionals over the Internet. A number of anonymous authentication schemes have been proposed in recent years to provide security in wireless body area networks. However, many of these systems are computationally inefficient during unsigned authentication. Additionally, previous schemes provided neither doctors nor patients with local secrecy. To overcome these limitations, this project proposes an efficient and secure framework for anonymous authentication using location privacy for IoT-based WBANs. A comprehensive analysis section shows that the proposed scheme overcomes the security weaknesses of existing schemes and also has a lower computational cost during anonymous authentication.

***Keywords**: Internet of Things (IoT), Wireless Body Area Networks (WBANs), security, computation cost, anonymous authentication, Time Division Multiple Access (TDMA), Access Points (APs), Media Access Control (MAC), 1-Round Anonymous Authentication Protocol (1-RAAP), Trusted authority (TA).*

I.Introduction

Wireless Body Area Networks (WBANs) have received a lot of public attention in recent years due to rapid advances in wireless technology. His IoT-based WBAN is designed to greatly support life by monitoring important parameters and the environment of the human body. Self-assembling WBANs can be formed using low-power medical sensors implanted in and around the human body. These sensors collect a patient's real-time biological information, such as blood pressure, heart rate, and pulse, and send the information to a remote medical server via his mobile device, such as a data sink. Based on the received information, the doctors and other medical experts can offer suitable clinical diagnostics to the patients. Since WBANs are used to afford proper and timely medical treatment to the patients, it is considered as a most welcomed technique for e-healthcare systems. In WBANs, the implanted sensors into the human body may communicate with each other and with the data sink. Similarly, the data sink can communicate with the remote service providers like doctors, medical consultants and the medical servers through hospitals. Hereafter, the disposition of WBANs in an IoT environment may well take care of the patients and the aged people by giving a robust and dependable health-monitoring service. Since the WBAN connects with more vital and sensitive patient associated information, it is necessary to offer security and privacy to this information. Moreover, privacy conservation is also an essential problem for a patient because biological information is considered to be highly intimate. Therefore, the biological information should be stored and conveyed secretly to prevent any information leakage to illegal users. Hence, it is very imperative to safeguard the patient-related information against security breaches and to confirm the patient’s privacy

The proposed framework is developed based on four security necessities:

(1) The privacy delivered by TA to WBAN users is a conditional privacy.

(2) The construction of our anonymous authentication framework is based on the use of bilinear pairing.

(3) In this proposed framework, TA is not required to keep the anonymous certificates of patients and medical experts. Instead, the patients and medical experts can make their own anonymous certificates to guard their privacy.

(4) In the case of any problem, TA has the facility to efficiently revoke the privacy of a misbehaving medical expert to discover its actual identity. Then, TA keeps actual identity of the revoked medical expert in its revocation list.

II) Related Work

In this proposed work to introduce a whole study of falls as pertinent situations. Here show an experiment of the fall-involved events of two types of falls based on an IoT prototype, the event patterns to detect the falls and their test using the IoT-TEG (IoT - Test Event Originator) tool. The fall analysis has highlighted the requirement to progress IoT-TEG with a new functionality which allows defining the anticipated conduct by defining behaviour rules [1].

We propose different mathematical models to evaluate IoT security based on port scan network presentation and IPsec services, which originates an optimal scan rate for sec-admins. The efficiency of the proposed framework is verified by wide-ranging numerical analysis, which shows that our approach reduces the risk to IoT devices while penetrating them at an optimal scan rate [2]

To implemented then validated the architecture using an onos sdn control and a raspbian virtual machine to discover how the proposed security machine mitigates malware packet injection ddos attacks using mirai spoofing masquerading and man-in-the-middle attacks did security and performance investigation of proposed security mechanisms and their applications [3]

A new framework model is proposed. Initially, a novel feature selection metric approach named CorrAUC proposed, and then based on CorrAUC, a new feature selection algorithm name Corrauc is develop and design, which is based on wrapper technique to filter the features accurately and select actual features for the selected ML algorithm by using AUC metric. Then, we applied combined TOPSIS and Shannon Entropy based on a bijective soft set to authenticate selected features for malicious traffic identification in the IoT network [
[4]

We evaluate our proposed method by using the Bot-IoT dataset and four dissimilar ML algorithms. Investigational results analysis showed that our proposed method is efficient and can achieve >96% results on average.
We design and implement a novel IoT interworking architecture providing a semantic driven addition framework appropriate for Smart City. The fundamental idea behind our approach is to introduce interworking proxies that (1) conduct a static mapping of sensor information between IoT platforms; (2) perform semantic interoperability using semantically glossed resources through a semantic interworking proxy that energetically discovers new kinds of information and adjusts itself to enable automatic translation of semantic data between given source and target IoT platforms although it is running [5]
This paper analyses the individualities of recently proposed off-body WBAN channels and bit error performances when the human body switches. In order to avoid insufficient channels and to improve the bit error performances, the receive antenna is attached to the back side, moreover. And the performance for each diversity system is evaluated [6]
We propose a modified super frame structure, in which separate admittance phases are introduced for the emergency event and regular event. In case of an emergency event, a novel emergency event handling outline and a ranking and priority assignment protocol is proposed to detect and address the critical event of in-body sensors. To minimize the impact, a scheduled access mechanism is proposed according to the criticality of the node. Performance analysis of the proposed in-body sensor MAC is done in positions of latency and overall power consumption, in case of both emergency and regular events.[7].
The IC also apparatuses a highly precise, sub-microsecond one-way time synchronization protocol which is used for time stamping the acquired data. The communication module was implemented in a 4-metal, 0.35 µm CMOS technology. The extreme data rate of the system is 35 Mbps while supporting up to 250 sensors, which exceeds current BAN applications scenarios[9]

The proposed system is applied with an irrelevant overhead. Two adaptive use bags, based on signal strength, are applied to demonstrate this system. First, the hub requirements the nodes with high signal strength to authorization convey support, and second, the hub requirements the nodes with low signal strength to set a sleeping pattern. In the first case, packet delivery rises significantly, while in the second case, each node saves an total of energy.[10]

in this paper, we've got proposed a trust-based verbal exchange scheme to assure the dependability and privacy of WBAN. To make sure reliability, a supportive verbal exchange method is used, at the same time as for privacy maintenance, a cryptography mechanism is used. The performance of the proposed scheme is evaluated the usage of MATLAB simulator. The output outcomes demonstrated that the proposed scheme increases facility delivery ratio, reliability, and agree with with reduced common put off. additionally, a fuzzy-good judgment approach used for ranking benchmark schemes that has been concluded that the proposed scheme has on top using comparative overall performance ranking [11].

An inexperienced electricity qos manage scheme for energy harvesting wban is proposed that guarantees the exceptional probably qos through successfully transmitting the information packets stochastic modelling of wirelessly powered wearable's proposed in four affords an analytical framework for the sns capability to notify the medical personnel approximately the affected individuals situation punctually in five a medium get entry to control mac layer protocol for wban is proposed that makes use of the csma tdma hybrid schemes to increase the lifetime and ee of sns with the aid of saving strength in 6 a mac protocol for wban is applied in this work that confirms qos and ee inside the power forced network by means of manner of dynamically enhancing the transmission slot which incorporates the electricity intake of the sns is faded obliging power harvesting-adaptive mac protocol proposed in 7 improves the wban performance in terms of take away ee and throughput via shifting its operation based totally mostly on the energy harvesting events [12].

We confirmed that because of the moving common clean out, KMR reached 0.27, suggesting that the attacker's guarantee raised from 50% to seventy 3% within the measured take a look at. Importantly, we additionally found that quantize parameters want to be decided on carefully, as KMR discount for Alice–Bob will usually have a tendency to lower Eve's KMR [13]

The proposed scheme is self-possessed of semi-tensor compressive sensing, hash function, Arnold scrambling and chaotic scrambling (SC-HAC). For the adaptiveness trouble, our machine makes use of semi-tensor compressive sensing to encrypt more than one indicators with special dimensions. [14].

the prevailing physiological signal based totally key settlement structures are constantly not able to balance the above and safety well. To overwhelm these troubles, we make efforts. One is that we attempt to improve the randomness of the Inter-Pulse-c programming language (IPI) from electrocardiograms in the guidance of digitizing physiological signals. And the alternative is that we attempt to apply the bloom filter in preference to lots of chaff factors to conceal the functions exchanged for key settlement. The comparative analysis and experiments designate that the proposed scheme can concurrently acquire high safety strength and occasional overhead [15].

III WIRELESS BODY AREA NETWORK (WBAN)

WBAN is real distinctive from a WSN. In a WSN, community generation is in most cases specific because the time period among the community initialization/restart to the point when the final sensor or the majority of sensor nodes perish. However, in a WBAN, each sensor node is awesome because of its particular characteristic. The fatigue of 1 sensor node may additionally cause community failure. As a importance, community life of a WBAN in this challenge is denoted because the time length between the initialization/restart of a WBAN to the factor while the first sensor node in the community exhausts.

3.1 Network Model

in this mission, here planned a WBAN with one controller and l sensor nodes on a human frame. The coordinator is positioned at the the front side of stomach even as the sensor nodes are organised within the exceptional elements of the human body. each direct transmission and useful transmission are allowed in the network. The sensor nodes deployed inside the predominant frame part may be selected as relay nodes because of their shorter distance from the coordinator.

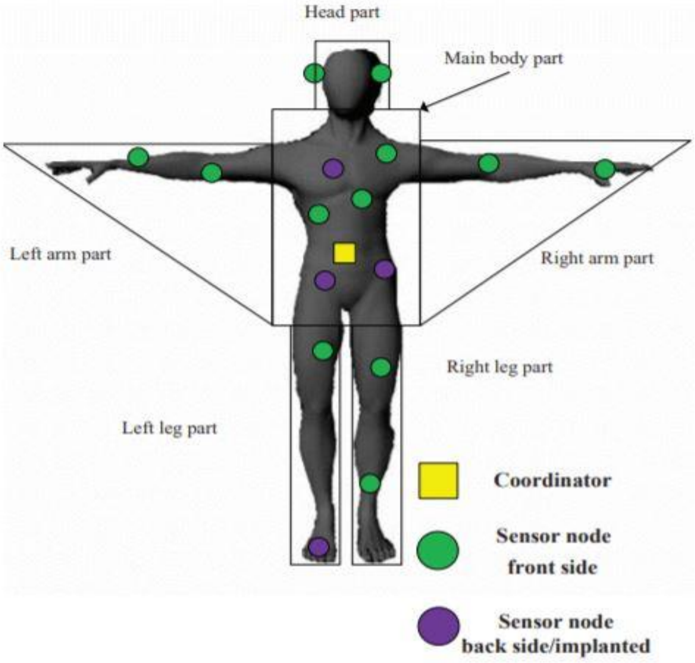


Fig 3.1. Network model.

Relay nodes must no longer simplest transmit their very own information to the coordinator, but additionally relay the facts from a few different nodes when decided on as bring. in addition, relay nodes are allowed to use direct transmission only to comply with the IEEE 802.15.6 two-hop tree topology constraint. most effective uplink statistics transmission from sensor nodes to the coordinator is considered because of utility scenarios like fitness monitoring wherein maximum of the statistics transmitted are sensed facts. right here anticipate that the coordinator is aware of the network topology and the gap between each pair of nodes consisting of it.

A easy Time division more than one access (TDMA) Media get entry to manage (MAC) is hired on this model to deal by way of multi-sensor transmission. be aware that this MAC is a commonplace used model of beacon-enabled first-rate frames MAC specified in IEEE 802.15.6. more precise, time is divided into superframes which has unchanging length. A superframe has two components: the energetic element and the inactive part. The energetic element consists of constant-duration time slots and each sensor node has one orthogonal time slot to ship its sensed information to the controller without wreck. If a sensor node is chosen as a relay, more time slots are prearranged to it. The range of the more time slots for a sure relay is decided by way of the number of relayed sensors it has. each sensor node transmits the sensed statistics to the receivers (both relay or the coordinator) in its dedicated slot, whereas relay nodes, if necessary, concentrate to their corresponding sensor nodes for records reception and transmits the relayed records together with their own facts to the coordinator in their allotted slots. for the duration of the motionless component, nodes fall asleep mode. when a WBAN units up or re-starts offevolved, the time slots allocation could be made by means of the coordinator relying at the communicate selection results. everyday sensor nodes are owed time slots first earlier than relay nodes. In in this task, it is meant that all nodes have enough sensed information to send throughout their allocated slots.**3.2 Architecture**

Generally, WBAN-based healthcare monitoring systems are composed of three tiers of communications

- Tier 1: Intra-WBAN communication
- Tier 2: Inter-WBAN communication
- Tier 3: Beyond-WBAN communication

Figure 1.1 gives an illustration on the working process of these three components. In tier 1 communication, bio-sensors, such as Electromyography (EMG) sensors, pulse oximeter, electroencephalogram (EEG) sensors, gather the life signals of human body and transmit these signals to a coordinator. In WBAN, this coordinator acts as a sink node, and communicates with all of the sensor nodes. A cell phone, or any other PDA, is generally a good choice for the role of coordinator. The coordinator should have access to the internet Access Point (AP). Once coordinator collects the data from the sensors, it will forward the data to the AP in tier 2 communication. In tier 3 communication, the life signal message will start from AP and be routed through the internet to the medical data centre, where doctors or auto-diagnose system will react to the irregular situations.

Tier 1: Intra-WBAN communication

in this degree, the communications inside the center of the body sensors and the communications among the body sensors and the coordinator is considered. The records transmission variety is around 2 meters in or round human frame. The community design in tier 1 is one of the maximum important studies recognition in WBAN, for the reason that Intra-WBAN communication wishes to resolve special assignment brought up by using the human body wi-fi conversation surroundings.

normally, for WBAN, superstar topology will paintings because the size of network is tiny. but, due to the low transmission strength and abnormal frame movements, amazing demanding situations exist or dependable wi-fi communications.Multi-hop network results in minor transmission energy, but better transmission delays. due to the fact the multi-hop community shortens the transmission distance, the facts transmission reliability can be improved. As proposed in the IEEE WBAN trendy, there can be at in particular two hops in IEEE WBAN requirements compliant communique. The cause is that, with the increase of the hopping wide variety, the conversation complexity and overhead may be accelerated as well. For a community with affordable length, a community design with greater than 2 degrees won't incur extra repayment.

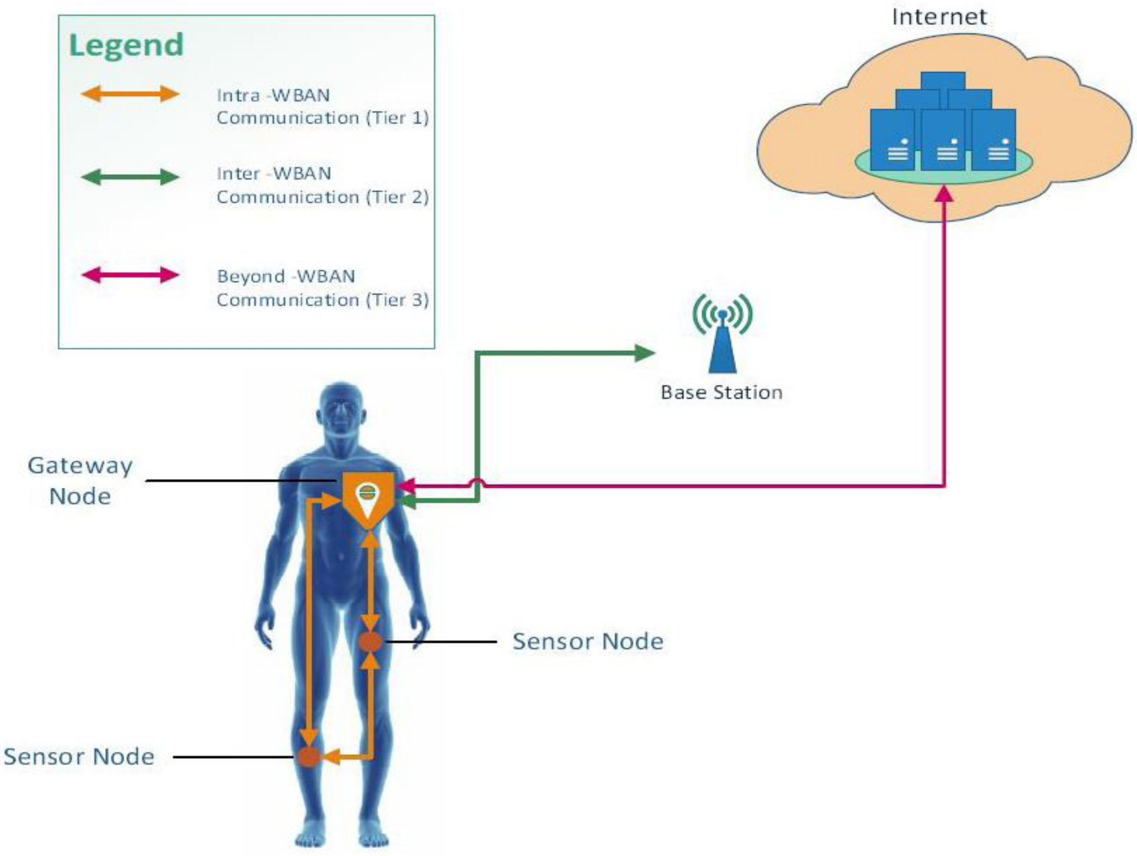

Legend
Intra -WBAN Communication (Tier 1)
Inter -WBAN Communication (Tier 2)
Beyond -WBAN Communication (Tier 3)
Internet
Base Station
Gateway Node
Sensor Node
Sensor Node

Fig 3.2: WBAN-based healthcare monitoring architecture

Tier 2: Inter-WBAN communication:

The aim for the communications in this layer is to connect the WBAN with the broader networks that we use each day in our each day lives, inclusive of the cell network and net. This connection is finished with the communique between the coordinator distinct in intra-WBAN, and one or greater get entry to factors (APs). The APs may be covered as part of the infrastructure, which is the infrastructure-based architecture, or may be located dynamically, that's the ad hoc-primarily based architecture.

Fig 3.3: Inter-WBAN Communication: Infrastructure-based architecture

A) Infrastructure-based architecture: The infrastructure-primarily based architecture is principal, as is proven in discern 1.2, and all the BANs in this location communicate with the equal AP. commonly, Inter-WBAN communication is restricted within a confined space, intended for instance, a waiting room within the sanatorium. The major advantage of the infrastructure-based architecture is that it permits for centralized management and security manipulate.

B) Ad hoc-based architecture: As is shown in discern 1.three, the ad hoc-based structure consists of a couple of APs, which forms a mesh structure. due to the function of advert hoc community, it permits for dynamic and bendy deployment. The community may be enlarged with minor have an impact on to the rest of the community. The multi-hop network guarantees large place coverage compared with the infrastructure-based structure, which greatly enables users's mobility.

Tier 3: Beyond-WBAN communication

past-WBAN communique considers the conversation between AP and the outdoor global, which includes net and far off electronic medical care centres. one of the cornerstones of Tier-3 is the database that stores user's profile and scientific records. The physician will get entry to to the affected person's records when wanted. automated notifications may be set to send emergency sound the alarm to each docs and patients while emergency reputation appears thru net or short message provider (SMS). any other prospective software scenario is remote disease diagnose as indicated in [3, 4, 13, 28]. The medical doctor can remotely gather all of the facts wished from the wireless sensors damaged with the aid of patient and the chronological data stored inside the database

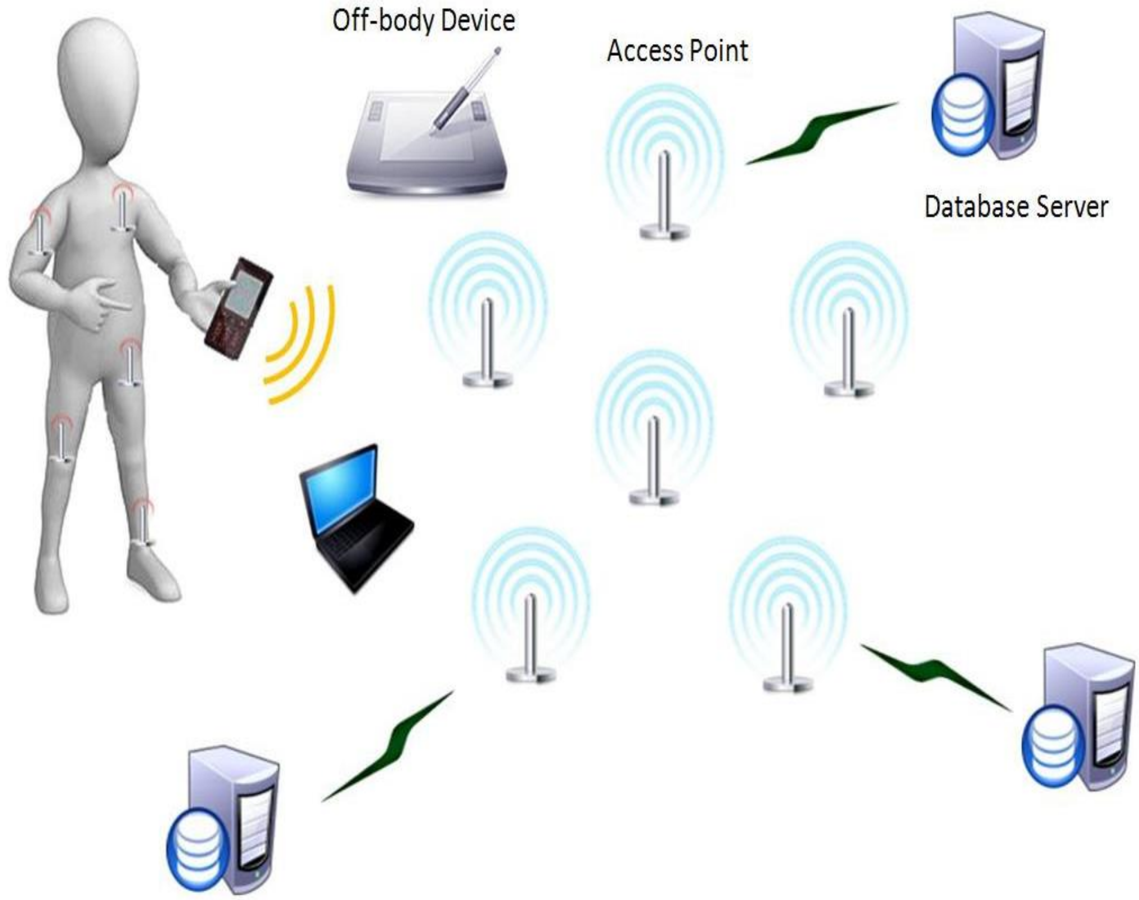


Fig. 3.4: Inter-WBAN Communication: Ad hoc-based architecture

3.3 Security model

In any device, designers make a hard and fast of assumptions about the machine and the entities that interact with it. as an example, designers make assumptions about the competencies of an adversary and the kind of threats adversaries might try to dedicate towards the device. here, kingdom those assumptions right here and outline those security goals our gadget achieves below those assumptions

A) Hardware capabilities

Here, make the subsequent assumptions about the form of hardware that is important to assist our gadget. The MN and SNs must have wireless competencies (e.g., 802.15.four, 802.eleven, or Bluetooth) and guide cryptographic primitives like encryption and authentication.

•here additionally assume the MN and SNs can securely pair; that is, they could authenticate each different and proportion keys using a pairing technique that uses the cryptographic primitives

•right here also count on the MN and SNs have some common sensor or sensors, like an accelerometer or gyroscope

.B) Trust assumptions

Right here outline consider to mean the ones assumptions that one entity has approximately every other entity. We make the subsequent assumptions about how the 3 entities – manufacturer, carrier provider, and users – believe each other in our machine. First, a person and the carrier provider agree with the manufacturer to provide calibrated SNs that perform effectively. This assumption permits users and service carriers to believe that the SNs are offering accurate facts. A person additionally trusts the provider company to no longer divulge the sensor facts it has obtained from the MN. The service issuer trusts the users to no longer tamper with the hardware or software program of the MN or the SN. The producer assumes nothing about any of the alternative entities.

C) Adversary model

Adversaries want to thwart the security of the machine. As such, we expect they have the subsequent skills that could allow them to attack the machine. We anticipate the adversary has the capacity to have a look at all (encrypted) messages at all times in the wireless medium. that is, they could study those messages being despatched between the MN and SNs. An adversary can use this capability, to discover the forms of SNs and MN in the system. We additionally anticipate the adversary has the ability to arbitrarily inject, adjust, and discard messages in the wireless medium. Accordingly, through disrupting a message and later re-injecting that message, they can also arbitrarily postpone or replay the message.

Right here additionally expect the following barriers approximately any adversary. First, we expect an adversary is computationally bounded, that means that it can't damage the cryptographic primitives without using a brute-force assault. 2nd, we assume an adversary will no longer access or alter the hardware nor alter the software of the MN or SN in our gadget. 0.33, we anticipate an adversary will not be capable of collect a topic’s biometric. Like a password, each challenge has an incentive to make sure their biometrics will now not be divulged to an adversary. sooner or later, we count on an adversary will not jam the wi-fi medium; this is, an adversary will no longer try to disrupt the usage of the device with the aid of acting denial-of-carrier assaults.

D) Security goals

The goal of our system is to permit users to put on an MN and SNs so one can acquire facts about their self and their surroundings and ahead this data to a carrier issuer for analysis in step with the believe assumptions. An adversary seeks to disrupt this process and acquire sensitive records in line with the risk model mentioned above. notwithstanding such an adversary, our machine must nevertheless obtain the subsequent dreams:

•Our machine must preserve the confidentiality of the sensed statistics and metadata. that is, the sensed information and its meta-facts have to now not be revealed to all people however the person and carrier company.

•Our system must keep the integrity of the sensed data and meta-data, that means that the service provider and person need to be able to believe that the sensed statistics or meta-statistics has no longer been tampered with.

•Our gadget must keep the authenticity of the sensed statistics and meta-records. that is, the service issuer need to be capable of trust that the sensed facts and meta-facts become received from the specified person and the required SN

•Our machine need to keep the obscurity of the sensors, meaning that the type of SN and MN the user is sporting have to no longer be revealed to every body however the person and the provider provider.

IV PROBLEM STATEMENT

In recent years, the WBAN has attracted quite a few attention from both the research network and industry as an critical part of the internet of factors (IoT). A WBAN includes many low electricity smart sensors, which might be placed in or across the human body. through those sensors, real-time tracking can be applied remotely. usual WBAN utility situation where the WBAN collects Realtime biomedical facts together with heart fee, blood strain, and pulse after which sends the data to a remote scientific server thru cell gadgets which include a non-public virtual assistant (PDA) or a smart phone. Primarily based in this data, medical doctors and different medical personnel ought to get an affected person’s repute and provide the appropriate medical diagnostics. Consequently, the use and deployment of WBANs ought to help us to attend to elderly human beings and patients by using providing a reliable and sturdy health-tracking carrier in the IoT surroundings. The data accrued or transmitted in WBANs are very sensitive and essential because these are the idea of scientific diagnostics. besides, privateers is also an essential trouble from the affected person’s perspective because biomedical statistics are incredibly confidential and have to be handled, transmitted, and saved with care to save you statistics leakage to unauthorized users. Furthermore, privateers’ renovation is likewise a crucial problem for a affected person due to the fact organic data is taken into consideration to be relatively exclusive. Consequently, the biological information must be saved and transmitted secretly to prevent any facts leakage to illegal users. For this reason, it's far very important to protect the patient-related information in opposition to security breaches and to ensure the patients privateers

V OBJECTIVE OF THE PROJECT

Based totally at the proposed demanding situations and issues, the primary contributions of our proposed green and secure nameless authentication framework are provided as follows.

(1) To advise a computationally efficient patient’s anonymous authentication framework that allows the authorized docs to check legitimacy of the patients in a comfy manner.

(2) To suggest an nameless physician’s authentication framework that allows the legal patients to verify the authenticity of the docs and medical experts in a secure manner.

(3) To assure privateness of the transmitted and saved information from unauthorized users of WBAN gadget.

(4) To make sure conditional privateness through which TA can revoke the unlawful docs or medical experts who abuse the WBAN system and to reveal their real identities to keep away from similarly unlawful sports.

(5) To offer area privateness the use of Chinese language remainder Theorem (CRT) to maintain the person's vicinity records secret from the unauthorized entities.

VI PROPOSED SYSTEM

Comparing with the previously proposed authentication and area privacy preserving schemes, the authentication scheme proposed in this challenge is extraordinary in 5 aspects. First of all, the proposed scheme preserves the real identities of patients and doctors from other users of the network in computational and communicational efficient way. Secondly, the integrity of the sensitive information is protected whilst the facts is exchanged between the patient and the medical doctor. Thirdly, a malicious consumer revocation mechanism is supplied to revoke the misbehaving users in WBAN system with low computational price. Fourthly, the confidentiality of the transmitted touchy records is preserved. Eventually, the region privacy of the sufferers is preserved from unauthorized entities within the network.

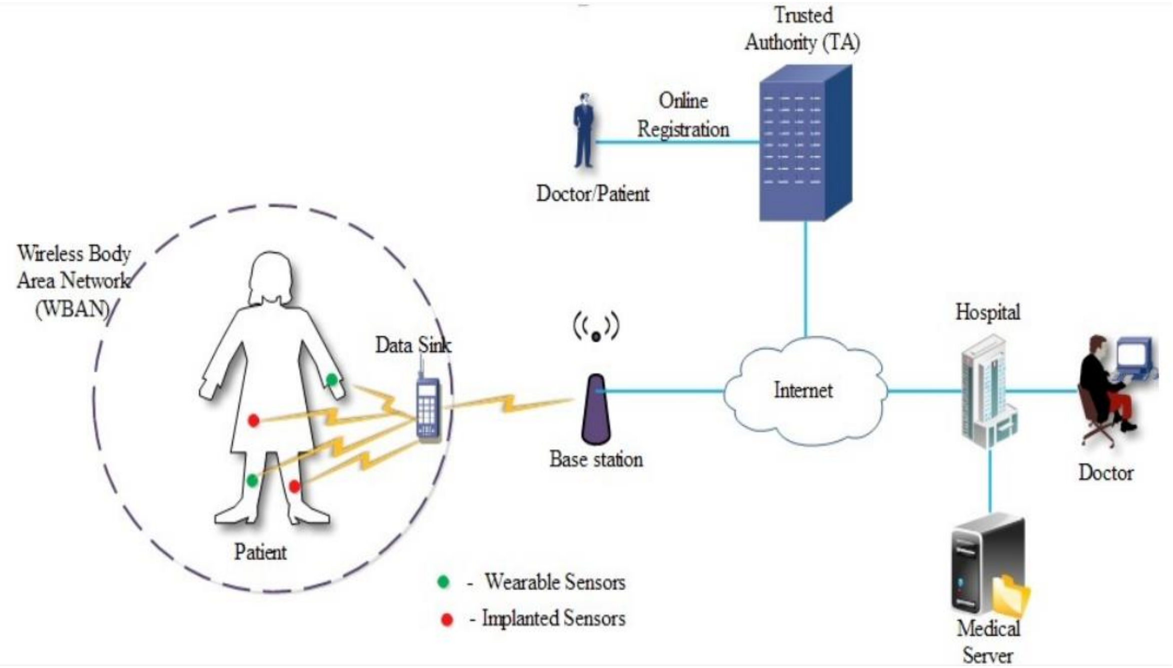
To offer this facility, in this project, an efficient anonymous authentication scheme for WBAN is proposed to deal with the hassle of safety and conditional privateness renovation in WBANs. In the anonymous authentication method, the sufferers can anonymously test the legitimacy of the health workers and the professionals can anonymously check the legitimacy of the patients earlier than sharing the biomedical facts with them. In case of any malicious conduct of an authorized scientific professional, consisting of imparting false information, or wrongly enhancing the contents of the patient reports, the relied-on authority (TA) can right away revoke the malicious expert from the WBAN machine. Considering the fact that low computational cost and clean revocation are the two vital homes of an green nameless authentication, on this task, a computationally efficient nameless authentication framework with conditional privateness keeping is proposed for WBANs.

Advantages of Proposed System

- Efficient and Secure
- Low computational cost
- resistance against attacks
- Low communication overhead
- Easily authenticate

• 7.2 System Architecture

•



• **Fig 5.1**: System Flow Diagram

- **Trusted authority (TA):**

The TA is used to do device initialization, public parameters generation, person registration and mystery keys generation for every consumer. The generated secret keys must be particular in nature to keep away from collusion assaults. Before everything, all customers are required to sign up inside the TA thru its internet site by using supplying the important facts, which includes non-public records, original identities and so on. A secure socket layer (SSL) encryption is performed among user and T A in the course of the registration procedure. After crowning glory of the registration system, TA problem credentials to the customers. Through getting the credentials from T A only, the users are considered as the WBAN customers.

- **Sensors:**

Commonly, a WBAN includes Wi-Fi wearable and implanted sensors. The wearable sensors are ready on/close to the surface human frame via wearable gadgets and the implanted sensors are implanted within the tissue of the human frame. These sensors are in particular used to offer life assist via tracking critical biological frame parameters together with blood stress, body temperature and so on. The main resource constraint of the implanted sensors is battery energy as compared to wearable sensors. Since the wearable devices are normally battery-powered, the batteries can be without difficulty modified and recharged. These wearable and implanted sensors acquire the statistics about the biological parameters of the human body and ship it to the facts sink. In flip, the records sink of the specific affected person sends the organic information to a licensed medical professional or a licensed health practitioner periodically.

- **Data Sink:**

A data sink is a cellular device together with a smartphone or a BAN controller that is used to accumulate the affected person’s biological information from the implanted and wearable sensors. The data sink has communication and computation competencies to send the organic information to the authorized doctors. The facts sink has the garage capability to store the accrued biological records and to store the secret keys that are given through T A during the time of user’s initial registration system. The records sink can authenticate the medical examiners or docs in an nameless manner to understand their legitimacy with T A earlier than sending the organic data to them, however, protecting the information inside the records sink is likewise critical to keep away from numerous classes of safety attacks in WBANs, in order to triumph over this hindrance, in our framework, the data is saved in an encrypted way and subsequently the attacker has no manner to get admission to the authentic record, therefore, the primary functionally of the facts sink is to maintain the information in an encrypted shape and to disseminate the data to the legal doctors or medical examiners additionally in an encrypted shape, consequently, the data stored in the facts sink is included and it isn't always without difficulty compromised by using attackers.

- **Users:**

The authorized patients, medical doctors or different health workers are considered as the users in the WBAN gadget. T A can generate a fixed of unique secret keys for each registered person, those keys are used to anonymously authenticate the sender of the patient-associated facts and to keep away from the malicious injection of information from the out of doors.

6.1 FEASIBILITY STUDY

Feasibility observe is the check of a machine concept in keeping with its workability, effect on the business enterprise, ability to satisfy user desires, and effective use of recourses. It specializes in the evaluation of present system and strategies analysis of alternative candidate system fee estimates. Feasibility analysis was done to determine whether the device could be possible.

The development of a laptop primarily based machine or a product is much more likely plagued by resources and transport dates. Feasibility study facilitates the analyst to decide whether or not or no longer to proceed, amend, postpone or cancel the venture, specifically vital while the assignment is big, complex and steeply-priced.

As soon as the analysis of the consumer requirement is complement, the system has to check for the compatibility and feasibility of the software program bundle that is aimed toward. The primary regions of feasibility analysis are:

- Technical Feasibility
- Financial Feasibility
- Resource Feasibility
- Operational Feasibility
- Economical Feasibility

Split Database Architecture

Microsoft get admission to applications can adopt a break up-database architecture. The database may be divided right into a front-quit database that built-in the application objects (queries, paperwork, reviews, macros, and modules), and is connected to tables saved built-in a lower back-cease shared database using the built-information. The "returned-quit" database can be saved built-in a place shared built-in many users, built-include a report server. The "the front-give up" database is sent to each consumer's computer and connected to the shared database. This design, each person has a replica of Microsoft get entry to integrate on their built-in alongside their software database. This reduces network visitors built-in utility isn't retrieved for every use, and built-in the front-quit database to integrated tables with built-integrated this is personal to each user for temporary facts. This split-database layout also lets built-in development of the application built-independent of the built-information. Whilst a new edition is prepared, the the front-stop database is changed without the built-in database. Microsoft get admission to have two database utilities, Database Splitter and related table manager, to facilitate this structure.

Connected tables integrated get right of entry to use absolute paths built-instead of relative paths, so the improvement built-in both has to have the equal route because the built-in a built-habitual can be written built-in VBA.

for very large get entry to databases, this may have overall performance problems and a sq. backend have to be taken this is less of an problem if the whole database can healthy built-integrated computer's RAM built-integrated get entry to caches and built-indexes.

VII Algorithm

In this phase, recommend a computationally green nameless authentication scheme based totally on bilinear pairing to avoid verbal exchange with malicious users inside the WBAN system. In nameless authentication, the sufferers can successfully authenticate the doctors without knowing their real credentials or identity statistics. Consequently, the privateers of the doctor is preserved from statistics leakage. Within the equal way, docs can anonymously authenticate the sufferers to keep away from communique with the malicious patients. To attain best nameless authentication, the person’s actual credentials and secret keys should be covered. Our scheme has six crucial levels particularly TA’s initialization, user registration, affected person’s nameless authentication procedure, health practitioner’s nameless authentication process, confidentiality and revocation.

A) Initialization:

TA picks the random numbers $t \in Z^* q$ as its master key and $a \in Z^* q$ as its private key. Then, T A computes its public key as $X_1 = g^{a\ 1}$ and an authentication parameter as $A_1 = g_1\ 2^{a+t\ 1}$.

B) User Registration

In the registration process, the WBAN users (patient or doctor or other medical expert) directly access the TA’s website and provides their personal details like name, address, mobile number and email id, etc.

1). If the user is the patient P_i , then T A gets the personal details from P_i and stores them in its database in a secure manner. Next, T A picks a random number $ui \in Z^* q$ and computes the private key as $P\ {}^rP_i = g_1{}^{ui+a}$

2) Then, T A generates an anonymous identity for each P_i such that $FP_i = g^{a+t-ui\ 1}$ to protect the real identity of P_i from unauthorized users during the time of communications. Instead of using the real credentials of P_i , the anonymous identity FP_i is used for communications in WBANs. Here, FP_i is mapped with the user’s real credentials only in TA. Therefore, by capturing this anonymous identity, it will give zero knowledge about the real credentials of Pi to attackers.

3) Besides, T A generates the tracking parameter TP_i such that $TP_i = g^{t+ui\ 1}$ for each Pi and keeps ($P\ kP_i$, $P\ rP_i$, FP_i , $T\ a\ P_i$) in its tracking list. In case of patient’s misbehaviouring, T A can revoke him/her from the WBANs using TP_i .

4) Then, T A sends P rP$_i$ through SSL to P$_i$ and P$_i$ stores P rP$_i$ in its data sink in a secure manner. Finally, T A sends Ω = ((FP$_i$ k P kP$_i$ k TP$_i$) ⊕ P rP$_i$) to P$_i$. By receiving this, Pi performs Ω ⊕ P rP$_i$ and gets (FP$_i$, P kP$_i$, TP$_i$).
5) Similarly, for a D$_i$, T A picks a random number d$_i$ ∈ Z * q and computes the private key as P rD$_i$ = g 1 d$_i$+a 1 and its corresponding public key as P kD$_i$ = g d$_i$ 1 .
6) Then, T A computes an anonymous identity FD$_i$ such that FD$_i$ = g a+d$_i$ 1 for D$_i$.
7) Moreover, the doctors are required to register their working medical institution in the TA. Then, T A generates an anonymous identity for the working institution of Di such that F$_{Mi}$ = g $^{a−di+t\ 1}$. Next, T A can generate this identity only if the corresponding medical institution is registered in the TA. The doctors of the non-registered institutions are not considered to be the part of the WBAN system. Hence, the medical institution is also anonymously authenticated by the patient.
8) For each Di , T A generates a tracking parameter TD$_i$ = g $^{t+di\ 1}$ and keeps (FD$_i$, F$_{Mi}$, T a D$_i$) in its tracking list to revoke the misbehaving doctors from the WBANs.
9) In addition, T A selects two secret keys (DSK) K$_{i1}$, K$_{i2}$ ∈ Z * q for a doctor D$_i$, where K$_{i1}$, K$_{i2}$ > 18000.
10) Next, T A sends P rDi through SSL to Di and the Di stores P rDi in a secure manner. Finally, T A sends Ω 0 = ((F$_{Di}$ || P k$_{Di}$ || F$_{Mi}$ || K$_{i1}$ || K$_{i2}$) ⊕ P rDi) to the Di . By receiving this, the Di performs Ω ‘ ⊕ P rD$_i$ and gets (FD$_i$, P kD$_i$, FM$_i$, K$_{i1}$, K$_{i2}$).

After the of completion of registration technique, a patient and a health practitioner can carry out nameless authentication manner.

C) Patient’s Anonymous Authentication Process

In nameless mutual authentication procedure, the sufferers and medical doctors are required to anonymously authenticate each different earlier than starting their communications. In affected person’s anonymous authentication procedure, the credentials of the patients are demonstrated anonymously by means of the doctors or the medical examiners.

Anonymous authentication certificates technology To prove the legitimacy to the doctors or medical experts anonymously, the affected person’s statistics sink first generates the nameless authentication certificates (AAC) as per the following steps:

Anonymous signature generation:

To hold the integrity of the verbal exchange messages, the data sink is required to generate the anonymous signature.

Anonymous signature verification:

By receiving {AS k $_m$ k δ1}, Di first verifies the integrity of m by checking whether e(δ1 × g b 1 , AS) = e(g1, g2). If this condition is satisfied, then Di accepts m, otherwise rejects it.

$$\begin{aligned} e(\delta_1 \times g_1^b, AS) \\ &= e(g_1^k \times g_1^b, g_2^{\frac{1}{k+b}}) \\ &= e(g_1^{k+b}, g_2^{\frac{1}{k+b}}) = e(g_1, g_2) \end{aligned}$$

Anonymous authentication certificate verification:

Next, D$_i$ checks the timestamp T S$_i$ such that |T $_{Sj}$ − T S$_i$ | < ∆T to avoid the replay attack where ∆T is the mutually agreed time delay between the Di and P$_i$.

$$\begin{aligned}\gamma_1' &= \delta_1 \times \mathcal{O}_1 \times \mathcal{O}_2 \\ &= g_1^k \times g_1^{l+\beta} \times g_1^{-l} \\ &= g_1^{k+l+\beta-l} \\ &= g_1^{k+\beta} = \gamma_1\end{aligned}$$

$$\begin{aligned}\gamma_2' &= \mathcal{O}_2 \times \mathcal{O}_3 \times \mathcal{O}_4 \\ &= g_1^{-l} \times g_1^{-\beta+l} \times g_1^{\alpha+l} \\ &= g_1^{-l-\beta+l+\alpha+l} \\ &= g_1^{-\beta+\alpha+l} = \gamma_2\end{aligned}$$

After verifying the anonymous signature and anonymous authentication certificate only the doctor Di can analyze the biological information (BI). If any one of the verification processes fails, then Pi is considered as the illegal user of WBAN system.

D) Doctor's Anonymous Authentication Process

before sending the biological information and getting the scientific advises or commands from the physician, it is essential for the patient to test the legitimacy of the medical doctors or health workers in an anonymous manner.

Doctor's anonymous authentication certificate generation:

D_i generates his authentication certificate DAAC as follows:

(a) Di computes an arbitrary parameter θ1 as θ1 = FMi × FDi .

(b) After computing θ1, Di computes a challenger value (DCV) as DCV = H(e(g1, g2)kFDi kP kDi).

(c) Then, Di sets its anonymous certificate as DAAC = {θ1, FDi , P kDi } and sends it to the data sink of Pi along with the timestamp T Si+1.

(d) By receiving this, Pi first verifies the current timestamp and then verifies whether e(θ1, A1) = e(g1, g2) to check the legitimacy of Di .

$$\begin{aligned}&h_1 \\ &\quad = e(\theta_1, A_1) \\ &\quad = e(F_{M_i} \times F_{D_i}, A_1) \\ &\quad = e(g_1^{a-d_i+t} \times g_1^{a+d_i}, g_2^{\frac{1}{2a+t}}) \\ &\quad = e(g_1^{a-d_i+t+a+d_i}, g_2^{\frac{1}{2a+t}}) \\ &\quad = e(g_1^{2a+t}, g_2^{\frac{1}{2a+t}}) = e(g_1, g_2)\end{aligned}$$

(e) Then, the data sink calculates its own challenger value as DCV 0 = H (h1 k FDi k P kDi) and compares whether DCV 0 = DCV . If these two values are equal, then the data sink considers that Di is an authenticated user of WBAN, otherwise, it simply avoids the future communications with Di.

At some point of the nameless authentication system as well as the communique of messages, the medical doctor does not know about the real place of the patient. The real region of the affected person is preserved from the alternative entities of WBAN by means of the TA. But, within the case of emergency, the health practitioner is needed to reveal the patient immediately.

Inside the case, the doctor can only get the region of the patient from TA using CRT-primarily based location privacy renovation procedure.

E) Confidentiality

After successful mutual authentication, the data sink of Pi sends the biological information (BI) to Di . To maintain confidentiality, the BI of Pi is encrypted by the data sink using any one of the ECC-based public key encryption algorithms.

$$\begin{aligned} C_1 \oplus H(e(Pr_{D_i}, C_2) \\ &= (Y \parallel BI \parallel Pk_{P_i} \parallel T_{P_i}) \\ &\quad \oplus H(e(g_1, g_1)^{r_i}) \oplus H(e(Pr_{D_i}, C_2) \end{aligned}$$

Where

$$\begin{aligned} H(e(Pr_{D_i}, C_2) \\ &= H(e(g_1^{\frac{1}{d_i+a}}, (Pk_{D_i} \times X_1)^{r_i})) \\ &= H(e(g_1^{\frac{1}{d_i+a}}, (g_1^{d_i} \times g_1^{a})^{r_i})) \\ &= H(e(g_1^{\frac{1}{d_i+a}}, (g_1^{d_i+a})^{r_i})) \\ &= H(e(g_1, (g_1)^{r_i})) \end{aligned}$$

Therefore,

$$\begin{aligned} C_1 \oplus H(e(Pr_{D_i}, C_2) \\ &= (Y \parallel BI \parallel Pk_{P_i} \parallel T_{P_i}) \oplus \\ &\quad H(e(g_1, g_1)^{r_i}) \oplus H(e(g_1, g_1)^{r_i}) \\ &= (Y \parallel BI \parallel Pk_{P_i} \parallel T_{P_i}) \end{aligned}$$

Similarly, Di sends his medical advise (MA) to Pi in an encrypted manner as follows

VIII. Result and Discussion

`On this section, endorse a computationally green nameless authentication scheme based on bilinear pairing to avoid verbal exchange with malicious customers inside the WBAN machine. In nameless authentication, the patients can effectively authenticate the medical doctors without understanding their real credentials or identity statistics. hence, the privateness of the medical doctor is preserved from records leakage. within the same way, docs can anonymously authenticate the patients to avoid conversation with the malicious sufferers. To acquire best anonymous authentication, the consumer's actual credentials and mystery keys should be covered. Our scheme has six important tiers namely TA's initialization, user registration, affected person's anonymous authentication system, physician's anonymous authentication system, confidentiality and revocation.**8.1**

Modules

- Setup Phase
- User Registration
- Patient's Anonymous Authentication Process

- Doctor’s Anonymous Authentication Process
- Confidentiality

Setup Phase

- TA picks the random numbers t ∈ Z ∗ q as its master key and a ∈ Z ∗ q as its private key.
- Then, TA computes its public key as X1 = g_1^a and an authentication parameter as A_1.
- TA picks secure cryptographic hash function H : {0, 1} ∗ → Z ∗ q and broadcasts {q, e, g1, g2, G1, G2, GT , X1, A1, H(·)} as the system parameters.

User Registration

- In the registration process, the WBAN users (patient or doctor or other medical expert) directly access the TA’s website and provides their personal details like name, address, mobile number and email id, etc.
- If the user is the patient Pi , then TA gets the personal details from Pi and stores them in its database
- Next, TA picks a random number and computes the private key and its corresponding public key
- Then, TA generates an anonymous identity for each Pi to protect the real identity of Pi from unauthorized users
- Besides, TA generates the tracking parameter for each Pi and keeps in its tracking list.
- In case of patient’s misbehaving, TA can revoke him/her from the WBANs using tracking parameter
- Moreover, the doctors are required to register their working medical institution in the TA
- TA can generate this identity only if the corresponding medical institution is registered in the TA
- Hence, the medical institution is also anonymously authenticated by the patient In addition, TA selects two secret keys for a doctor Di
-

Patient’s Anonymous Authentication Process

- In anonymous mutual authentication process, the patients and doctors are required to anonymously authenticate each other before starting their communications.
- In patient’s anonymous authentication process, the credentials of the patients are verified anonymously by the doctors or the medical experts
-

A) Anonymous authentication certificate generation

- To prove the legitimacy to the doctors or medical experts anonymously, the patient’s data sink first generates the anonymous authentication certificate (AAC)
-

B) Anonymous signature generation

- To maintain the integrity of the communication messages, the data sink is required to generate the anonymous signature as AS.
- By computing AS, the data sink sends to doctor Di

C) Anonymous signature verification

- By receiving anonymous signature, Di first verifies the integrity of m by checking whether condition.
- If this condition is satisfied, then Di accepts m, otherwise rejects it.

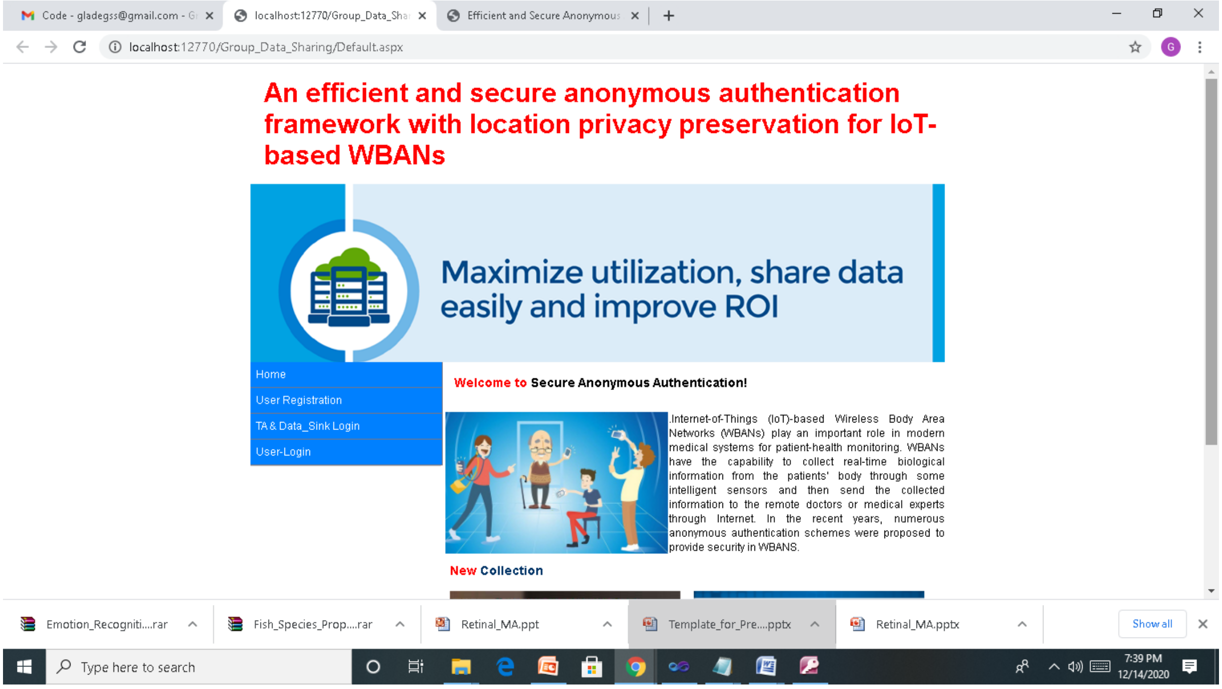
Doctor's Anonymous Authentication Process

- Before sending the biological information and getting the medical advises from the doctor, it is necessary for the patient to check the legitimacy of the doctors or medical experts in an anonymous manner.
- During the anonymous authentication, the doctor does not know about the real location of the patient
- The real location of the patient is preserved from the other entities of WBAN by the TA
- However, in the case of emergency, the doctor is required to monitor the patient directly
- In the case, the doctor can only get the location of the patient from TA using CRT-based location privacy preservation process.

Confidentiality

- After successful mutual authentication, the data sink of Pi sends the biological information (BI) to Di .
- To maintain confidentiality, the BI of Pi is encrypted by the data sink using any one of the ECC-based public key encryption algorithms.

Home Page



localhost:12770/Group_Data_Sharing/Default.aspx

An efficient and secure anonymous authentication framework with location privacy preservation for IoT-based WBANs

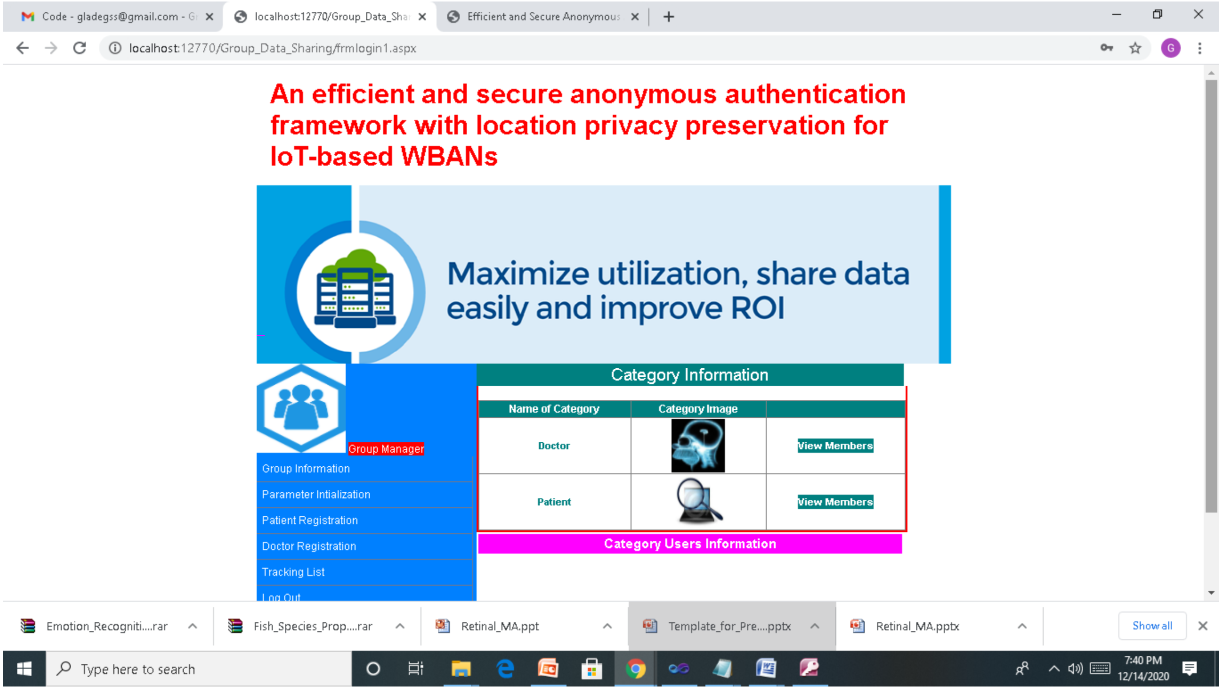
Maximize utilization, share data easily and improve ROI

Welcome to Secure Anonymous Authentication!

.Internet-of-Things (IoT)-based Wireless Body Area Networks (WBANs) play an important role in modern medical systems for patient-health monitoring. WBANs have the capability to collect real-time biological information from the patients' body through some intelligent sensors and then send the collected information to the remote doctors or medical experts through Internet. In the recent years, numerous anonymous authentication schemes were proposed to provide security in WBANS.

New Collection

Fig 8.1: Category Information



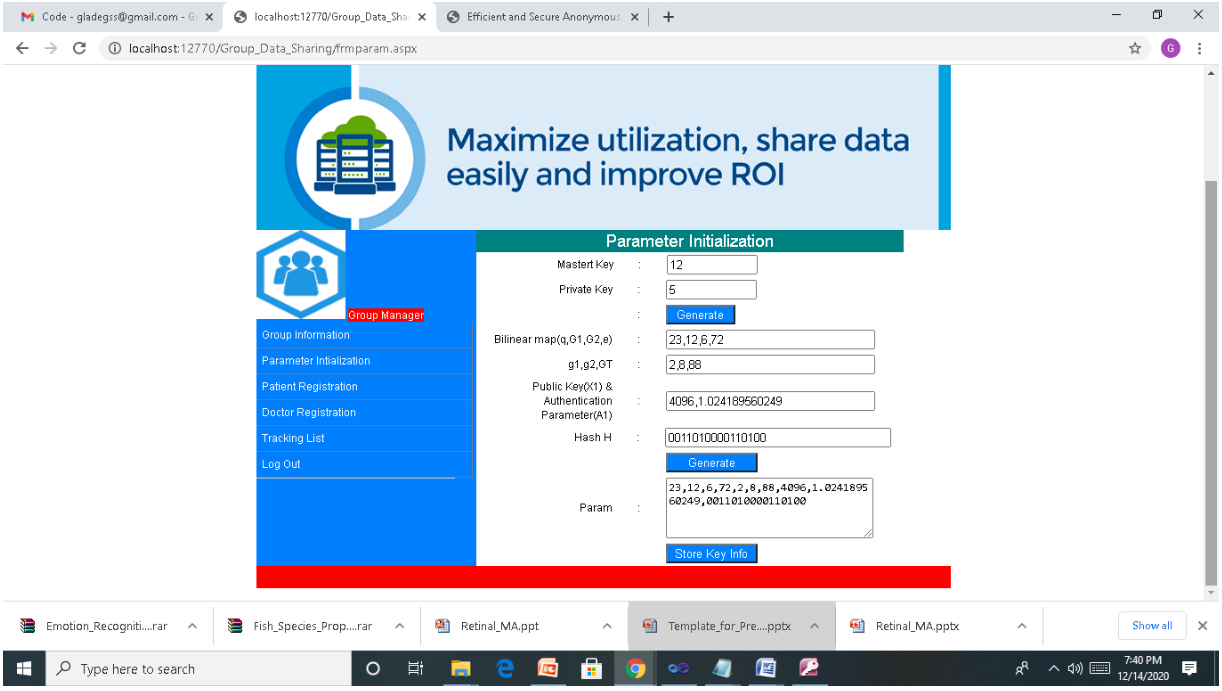
An efficient and secure anonymous authentication framework with location privacy preservation for IoT-based WBANs

Category Information

Name of Category	Category Image	
Doctor		View Members
Patient		View Members

Category Users Information

Fig 8.2: Parameter Initialization



Parameter Initialization

Mastert Key : 12

Private Key : 5

: Generate

Bilinear map(q,G1,G2,e) : 23,12,6,72

g1,g2,GT : 2,8,88

Public Key(X1) & Authentication Parameter(A1) : 4096,1.024189560249

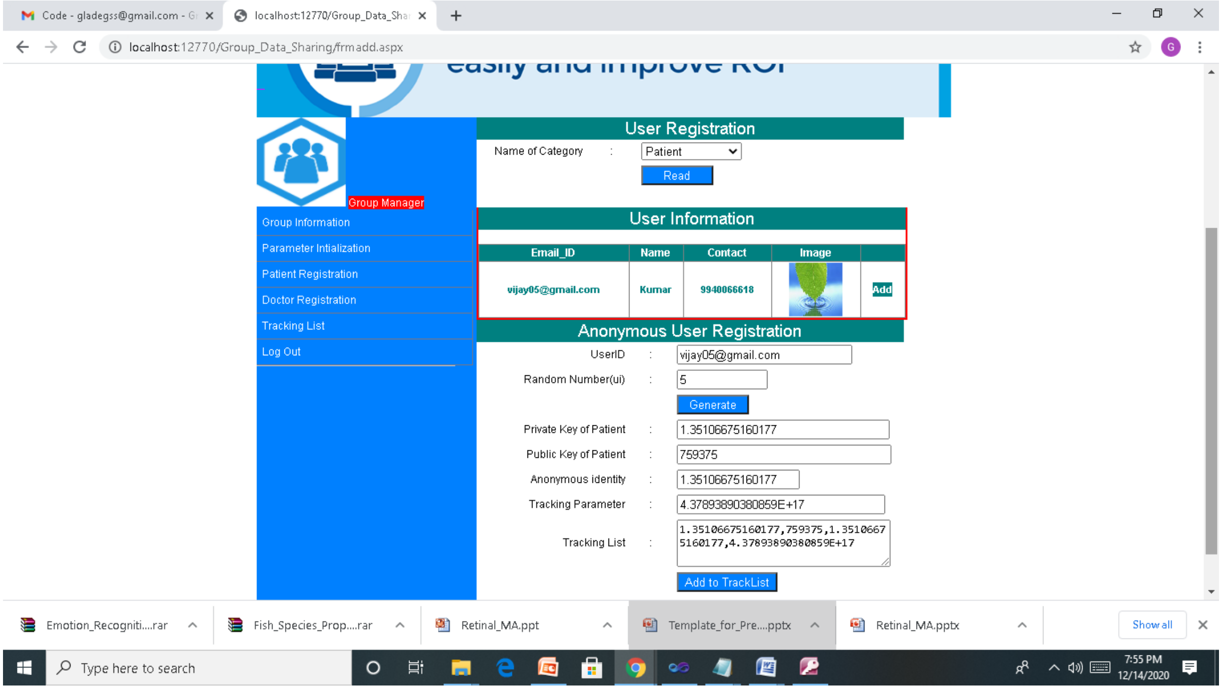
Hash H : 0011010000110100

Generate

Param : 23,12,6,72,2,8,88,4096,1.024189560249,0011010000110100

Store Key Info

Fig 8.3: Patient Registration



User Registration

Name of Category : Patient

Read

User Information

Email_ID	Name	Contact	Image	
vijay05@gmail.com	Kumar	9940066618		Add

Anonymous User Registration

UserID : vijay05@gmail.com

Random Number(ui) : 5

Generate

Private Key of Patient : 1.35106675160177

Public Key of Patient : 759375

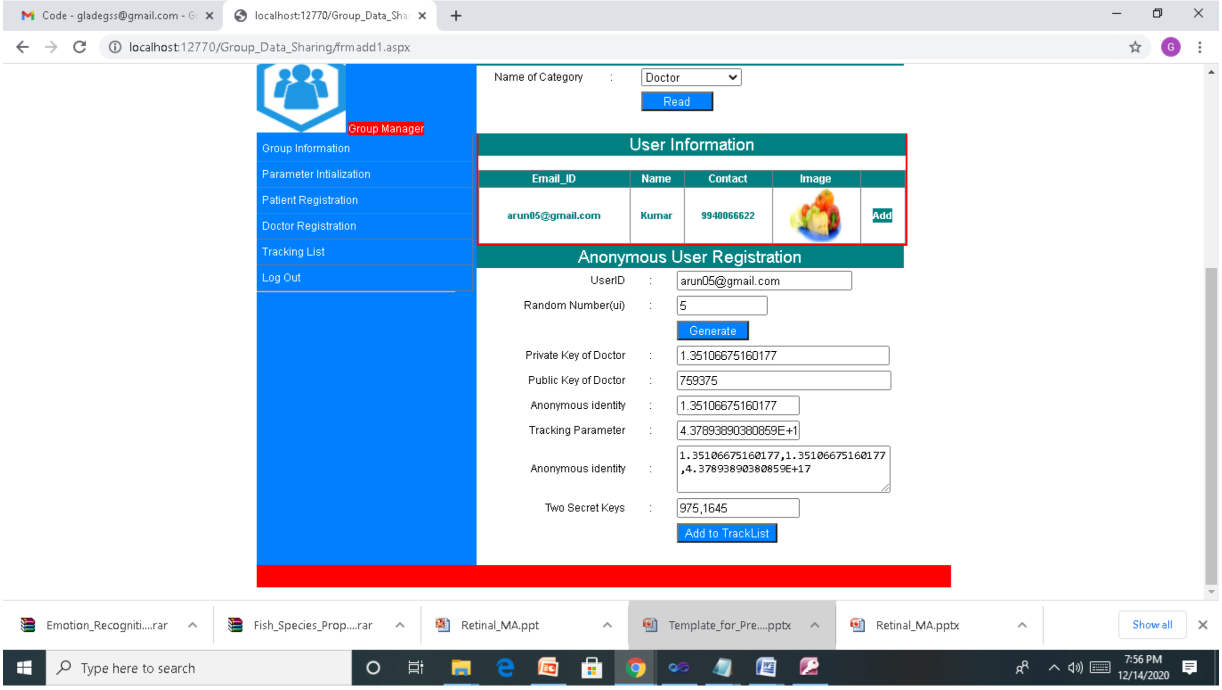
Anonymous identity : 1.35106675160177

Tracking Parameter : 4.37893890380859E+17

Tracking List : 1.35106675160177,759375,1.35106675160177,4.37893890380859E+17

Add to TrackList

Fig 8.4 Doctor Registration



Name of Category : Doctor

Read

User Information

Email_ID	Name	Contact	Image	
arun05@gmail.com	Kumar	9940066622		Add

Anonymous User Registration

UserID : arun05@gmail.com

Random Number(ui) : 5

Generate

Private Key of Doctor : 1.35106675160177

Public Key of Doctor : 759375

Anonymous identity : 1.35106675160177

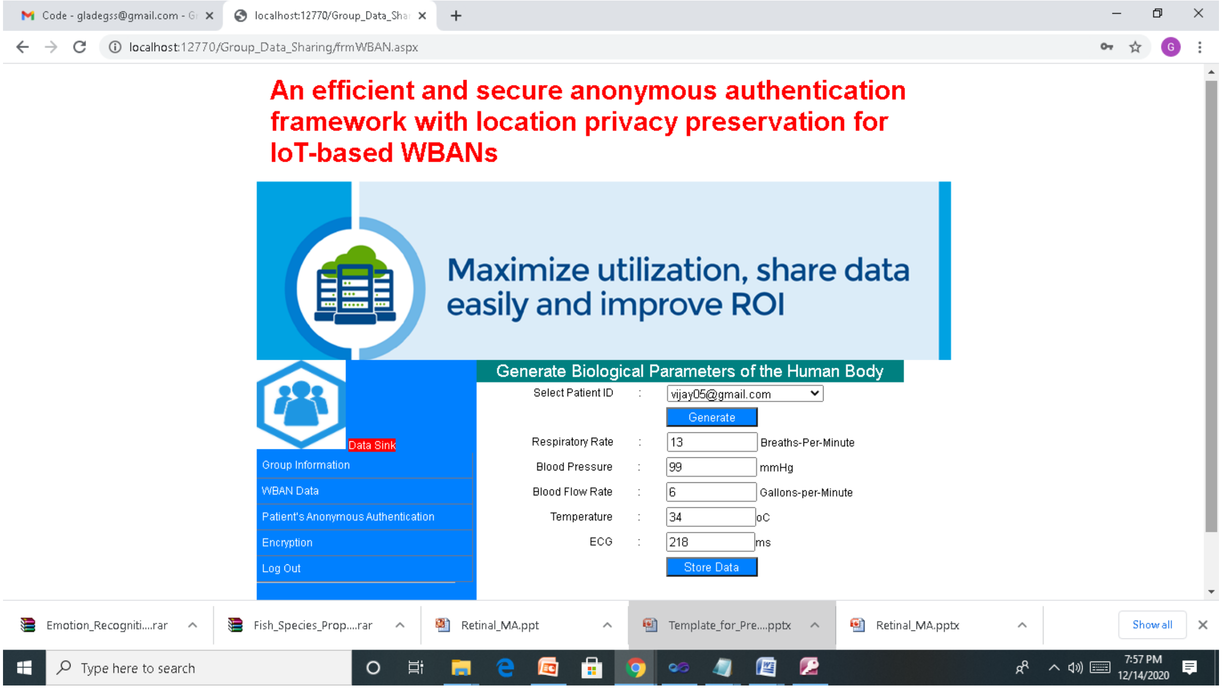
Tracking Parameter : 4.37893890380859E+1

Anonymous identity : 1.35106675160177,1.35106675160177,4.37893890380859E+17

Two Secret Keys : 975,1645

Add to TrackList

Fig 8.5 : Biological Parameters



localhost:12770/Group_Data_Sharing/frmWBAN.aspx

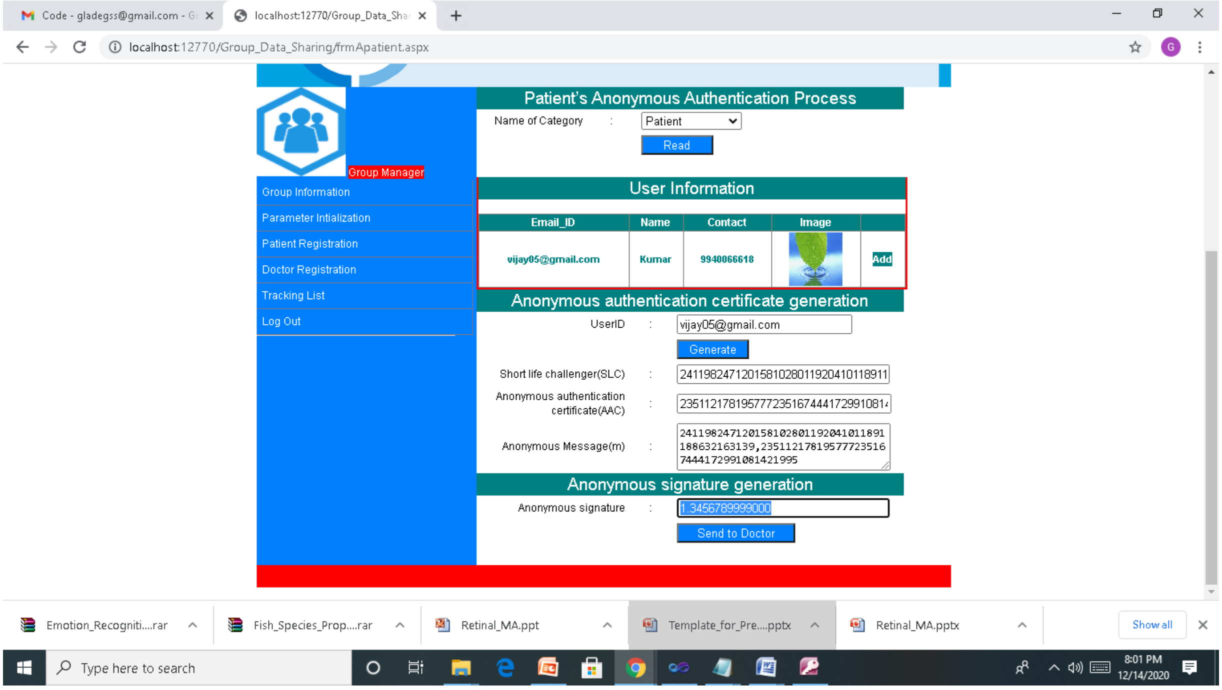
An efficient and secure anonymous authentication framework with location privacy preservation for IoT-based WBANs

Data Sink

- Group Information
- WBAN Data
- Patient's Anonymous Authentication
- Encryption
- Log Out

Generate Biological Parameters of the Human Body

Select Patient ID :	vijay05@gmail.com	
	Generate	
Respiratory Rate :	13	Breaths-Per-Minute
Blood Pressure :	99	mmHg
Blood Flow Rate :	6	Gallons-per-Minute
Temperature :	34	oC
ECG :	218	ms
	Store Data	



localhost:12770/Group_Data_Sharing/frmApatient.aspx

Group Manager

- Group Information
- Parameter Intialization
- Patient Registration
- Doctor Registration
- Tracking List
- Log Out

Patient's Anonymous Authentication Process

Name of Category : Patient

Read

User Information

Email_ID	Name	Contact	Image	
vijay05@gmail.com	Kumar	9940066618		Add

Anonymous authentication certificate generation

UserID : vijay05@gmail.com

Generate

Short life challenger(SLC) : 241198247120158102801192041011891

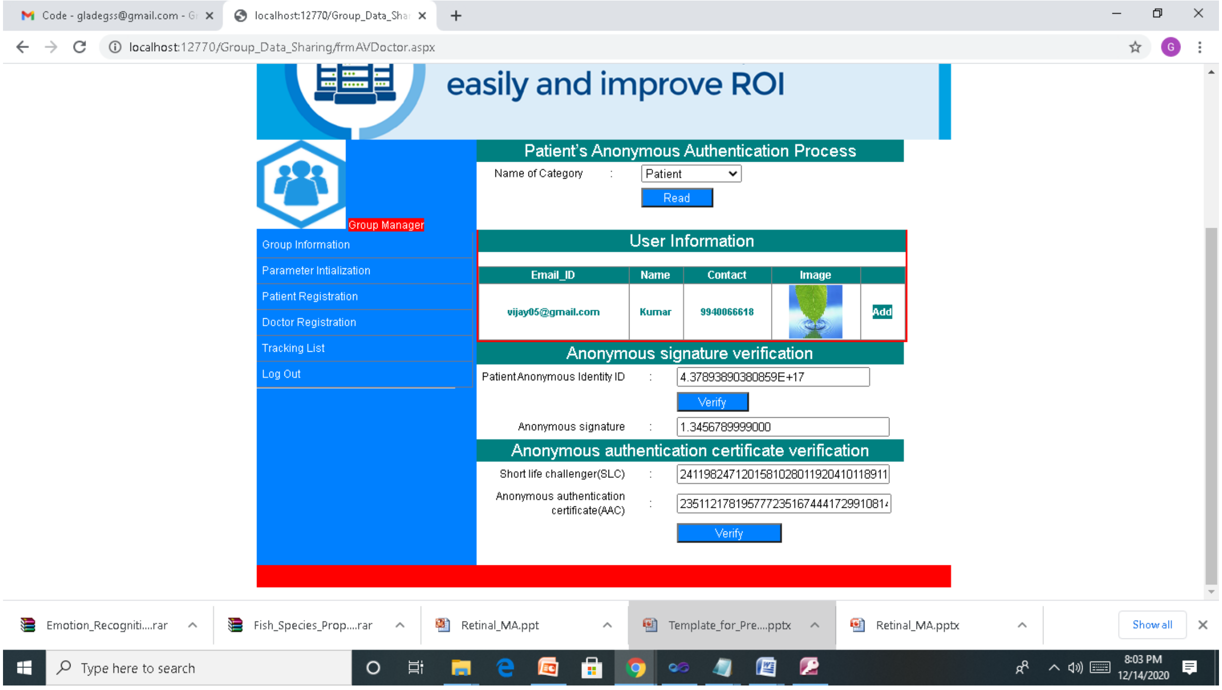
Anonymous authentication certificate(AAC) : 23511217819577723516744417299108l4

Anonymous Message(m) : 241198247120158102801192041011891188632163139,235112178195777235167444172991081421995

Anonymous signature generation

Anonymous signature : 1.3456789999000

Send to Doctor



Patient's Anonymous Authentication Process

Name of Category : Patient

User Information

Email_ID	Name	Contact	Image	
vijay05@gmail.com	Kumar	9940066618		Add

Anonymous signature verification

Patient Anonymous Identity ID : 4.37893890380859E+17

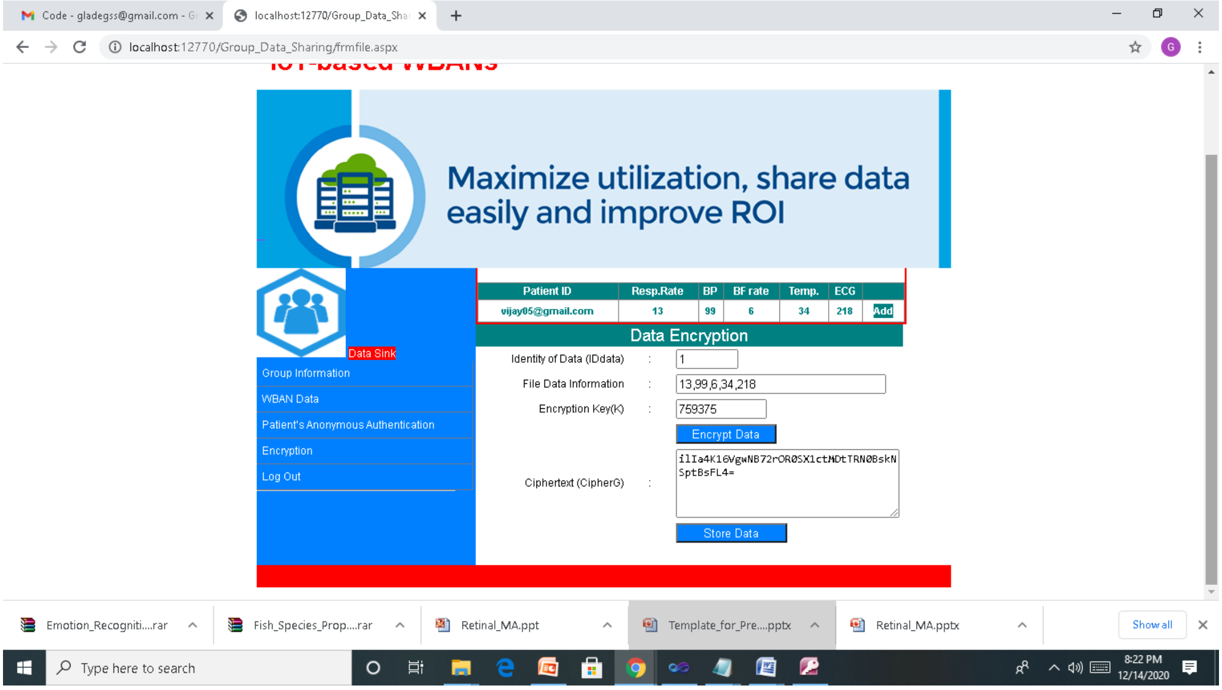
Anonymous signature : 1.3456789999000

Anonymous authentication certificate verification

Short life challenger(SLC) : 2411982471201581028011920410118911

Anonymous authentication certificate(AAC) : 235112178195777235167444172991081

Fig 8.6 : Data Encryption



localhost:12770/Group_Data_Sharing/frmfile.aspx
Maximize utilization, share data easily and improve ROI
Data Sink
Group Information
WBAN Data
Patient's Anonymous Authentication
Encryption
Log Out
Encrypt Data
Store Data

Patient ID	Resp.Rate	BP	BF rate	Temp.	ECG	
vijay05@gmail.com	13	99	6	34	218	Add

Data Encryption

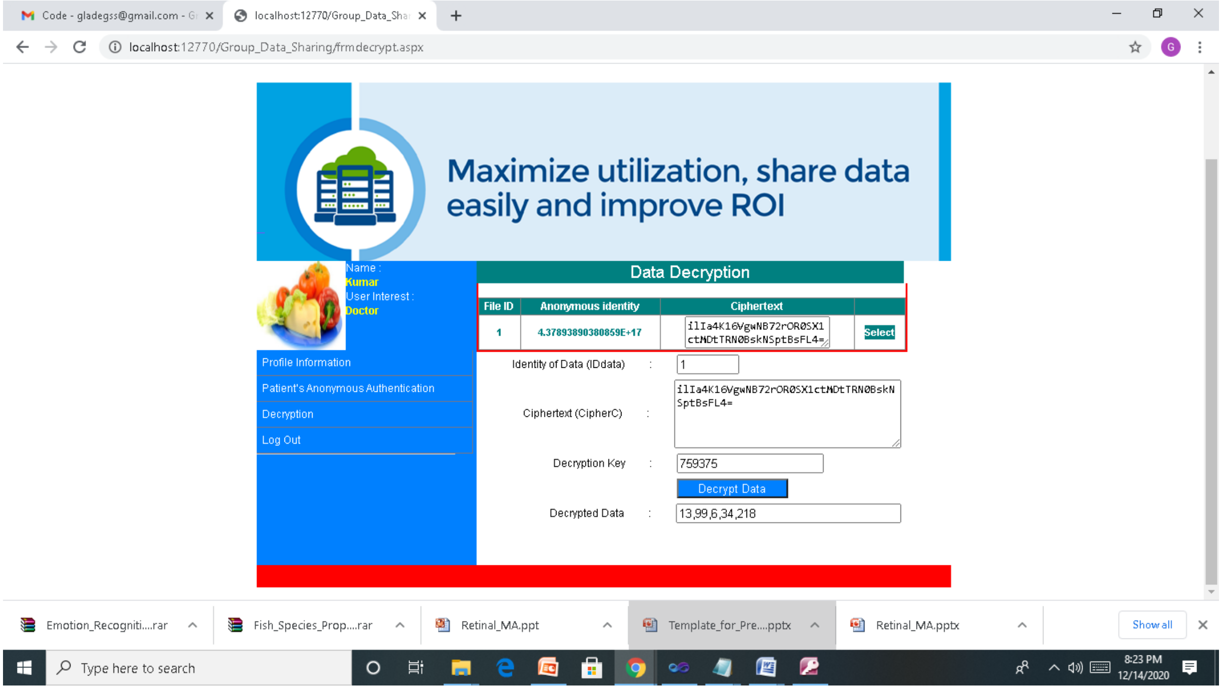
Identity of Data (IDdata) : 1

File Data Information : 13,99,6,34,218

Encryption Key(K) : 759375

Ciphertext (CipherG) : ilIa4K16VgwNB72rOR0SX1ctMDtTRN0BskNSptBsFL4=

Fig 8.7 : Data Decryption



Name : Kumar

User Interest : Doctor

Data Decryption

File ID	Anonymous identity	Ciphertext	
1	4.37893890380859E+17	ilIa4K16VgwNB72rOR0SX1ctMDtTRN0BskNSptBsFL4=	Select

Identity of Data (IDdata) : 1

Ciphertext (CipherC) : ilIa4K16VgwNB72rOR0SX1ctMDtTRN0BskNSptBsFL4=

Decryption Key : 759375

Decrypted Data : 13,99,6,34,218

IX. CONCLUSION

In this project, proposed an efficient and at ease nameless authentication framework with vicinity privatises maintenance for IoT-based totally WBANs. In our scheme, first the doctor anonymously authenticate the patient to check the patient's legitimacy after which the affected person anonymously authenticate the health practitioner to test the legitimacy of the medical doctor. Furthermore, the place privacy of both the patient and the physician is preserved by TA and it's miles exposed to the authorized doctors or sufferers based totally on using CRT. The safety analysis suggests that our scheme can offer resistance against impersonation assault, message change attack, replay assault, eavesdropping attack and man-in-the-center attack. The overall performance evaluation suggests that our scheme is green in terms of computational cost and subsequently it is greater suitable for sensible IoT-based totally WBAN programs.

X. FUTURE ENHANCEMENT

The destiny extension of this paintings is to offer the batch authentication to the communicating customers in a green way.

REFERENCES

1) Lorena Gutierrez-Madro, Luigi La Blunda et al.," Test event generation for a fall-detection IoT system" This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2909434, IEEE Internet of Things Journal
2) Shikhar Verma.,'' A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices'', IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 10, MAY 15, 2021.
3) Kallol Krishna Karmakar, Vijay Varadharajan et al.,'' SDN Enabled Secure IoT Architecture'', This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.3043740, IEEE Internet of Things Journal.
4) Muhammad Shafiq, Zhihong Tian et al.,'' CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques'' , This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.3002255, IEEE Internet of Things Journal.
5) JongGwan An, Franck Le Gall, Jaeho Kim et al.," Towards Global IoT-enabled Smart Cities Interworking using Adaptive Semantic Adapter'', IEEE INTERNET OF THINGS JOURNAL, VOL. , NO. , 2019.
6) Sang-Hun Han and Sang Kyu Park,'' Performance Analysis of Wireless Body Area Network in Indoor Off-body Communication'' , IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.
7) Sudip Misra, Pradyumna Kumar Bishoyi et al.,'' i-MAC: In-Body Sensor MAC in Wireless Body Area Networks for Healthcare IoT'', IEEE SYSTEMS JOURNAL.
8) Fardin Derogarian Miyandoab et al.,'' A Multifunctional Integrated Circuit Router for Body Area Network Wearable Systems'', IEEE/ACM TRANSACTIONS ON NETWORKING.
9) Fardin Derogarian Miyandoab et al.,'' A Multifunctional Integrated Circuit Router for Body Area Network Wearable Systems'', IEEE/ACM TRANSACTIONS ON NETWORKING.
10) Costas Michaelides and Foteini-Niovi Pavlidou.,'' Programmable MAC in Body Area Networks, One Command at a Time'', VOL. 3, NO. 7, JULY 2019.
11) Gulzar Mehmood , Muhammad Zahid KHAN et al.,'' A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks '', This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3007405, IEEE Access.
12) Osama Amjad, Ebrahim Bedeer , and Salama Ikki., '' Energy Efficiency Maximization of Self-Sustained Wireless Body Area Sensor Networks '', This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LSENS.2019.2946851, IEEE Sensors Letters.

13) Ruslan Dautov and Gill R Tsouri, ‘’ Effects of Passive Negative Correlation Attack on Sensors Utilizing Physical Key Extraction in Indoor Wireless Body Area Networks ‘’, VOL. 3, NO. 7, JULY 2019.

14) Lixiang Li, Lifei Liu, Haipeng Peng, Yixian Yang, and Shizhuo Cheng.,’’ Flexible and Secure Data Transmission System based on Semi-Tensor Compressive Sensing in Wireless Body Area Networks’’, This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2881129, IEEE Internet of Things Journal.

15) Xuanxia Yao, Wanyou Liao, Xiaojiang Du et al., ‘’ Using Bloom Filter to Generate a Physiological Signal based Key for Wireless Body Area Networks’’ , JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015.

BIBILOGRAPHY

Books

- Jason Butlre and tony Caudil, ”ASP.NET Database Programming” Fifth Edition, Hungry minds, Inc.Publicating Company Limited, New Delhi, 2000.
- Glen Johnsonwiley, Learning ASP.NET , Fourth Edition, Hungry minds, Inc. Publicating Company Limited, Uttar Pradesh, 2001.
- Jason Butlre and tony Caudil, ”ASP.NET Database Programming” Second Edition, Hungry minds, Inc.Publicating Company Limited, New Delhi, 2000.
- K.M. Hussian and Donna Hussaian, Information Systems: Analysis, Design and implementation, Second Edition, Tata McGraw-Hill, Delhi, 1995.
- Edward Yourdon, Managing the System Life Cycle, Second Edition, Englewood cliffs & N.J, Yourdon Press, US, 1989.
- Edward Yourdon and Larry L. Constantine, Structured Design: Fundamentals and Applications in Software Engineering, Second Edition, Englewood Cliffs & N.J, Yourdon Press, US, 1989.
- Shaku Atre, Data Base: Structured Techniques for Design, Performance and Management, Third Edition, Wiley, New York,1980.
- J.D.Lomax and Rochell Park, Data Dictionary Systems, NCC Publications,1977.