Multimedia Tools and Applications (2023) 82:453–478
https://doi.org/10.1007/s11042-022-13310-3

Safeguards and weightless of electronic chain of command consolidated for virtual patient evaluation

Mohammed Imtyaz Ahmed[1] · G. Kannan[1]

Received: 25 March 2021 / Revised: 7 February 2022 / Accepted: 30 May 2022 /
Published online: 7 June 2022

Abstract

The Internet of Things (IoT), 5G cellular technology, and Cyber-Physical Systems (CPS) are enabling a wide range of IoT-based application cases that are both intelligent. As one of the most impactful applications of the Internet of Things (IoT), healthcare makes use of AAL (Ambient Assisted Living), mobile health (mHealth), and electronic health (eHealth). Spending on health is a significant portion of people's income. Traditional medicine is prone to long delays, waste of money and effort, and even death. RVO (Remote Victim Observation) can be utilized to circumvent problems associated with traditional healthcare facilities because of IoT's intelligence and predictive power. With the help of IoT-based RVO and wearable devices, sensor networks, and other digital infrastructure, we can detect oncoming situations before they become life-threatening or even fatal. IoT integration with healthcare units was demonstrated in order to build a trustworthy, available, and secure RVO system. Secure end to end communication, encryption of RFID data, and privacy protection are all part of the proposed solution. An android wearable watch (Biosensor | Body sensor), a server using REST framework, and a smartphone app to monitor and detect falls, blood pressure, and heart rate are all part of the system. As a bonus, the peace and quiet of this secluded location contribute to the attraction. Using this RVO could improve health care and quality of life, according to an empirical investigation.

Keywords IoT · Medicalcare · Biosensors · Security · Privacy · Remote victim observation

✉ Mohammed Imtyaz Ahmed
mdimtyazahmed@gmail.com

G. Kannan
kannann@crescent.education

[1] ECE Dept, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

1 Introduction

Rapid advances in mobile and networking technology have resulted in numerous new and exciting applications. They use Wi-Fi, 4G LTE, Zigbee, and Bluetooth wireless communication in their programmes. These are the most commonly used mobile gadgets in daily life. A service like remote medical monitoring and care is described in Moosavi et al. [29] and Simplicio et al. [38]. Several countries have recently launched programmes to address the growing healthcare needs of an ageing population. A full medical network can be built using wireless technology, sensors, actuators and the internet of things Yang et al. [48]. It's interaction with the internet of things will improve future medical and healthcare applications Ray et al. [34].

To protect medication administration and tracking, the medical industry currently relies on IT. Radio Frequency Identification (RFID) is employed in this process. Blood samples and other medical data can all be recognised using this method in a novel manner. The elderly and children, as well as many other real world scenarios Simplicio et al. [39], Chiuchisan et al. [9], Khemissa et al. [23], Yang et al. [46] and Imtyaz Ahmed et al. [4], can be properly monitored through the use of various real-world instances. Better medical care will be required as the world's population ages. Therefore, it is critical that these folks obtain medical attention without having to visit a hospital. Extended and distant medical monitoring can be made possible by the use of mobile healthcare services, GPS location, rural medical care, wheelchairs, and other equipment and technology that makes this possible.

As technology has advanced, physiologic sensing devices have kept pace. Devices like this one are smaller and more power efficient. As a result, they are suitable for long-term body sensing in wearable devices. Personal wireless devices are connected to sensors on the body via the body area network (BAN), as seen in Lee et al. [25], Abbas et al. [2], Liang et al. [27], Yang et al. [47] and G Kannan et al. [22]. The recent advancements in Internet of Things (IoT) technology have made it possible to integrate healthcare services and enable remote healthcare monitoring in near real time. This study analyses a stimulating setting in order to reach this goal. Personal wireless devices integrated with sensors can be used to collect and send physiological data from victims. This information can be used for both diagnosis and treatment by medical experts.

A third party reader can access the wearable device's data. Victims' medical records will be more readily available to medical professionals, regardless of where they are located: in the hospital or at home. Body sensors send data to a device or data reader Chen et al. [18], Han et al. [16], Zhao et al. [52] and Whitmore et al. [44]. Medical workers can gather and communicate victim data, which can then be used by doctors to diagnose and treat victims. Governments at all levels can benefit from this data, including the federal government. Wearable sensors generate a great deal of "big data," which is referred to as the volume of data they collect on a regular basis. Cloud computing and cloud based distributed programming frameworks must be employed in order to process this data.

BodyCloud was proposed by Fortino et al. [11] as a name for a body sensor network (BSN). An internet protocol was designed to communicate with a network of body sensors. C-SPINE a BSN architecture was introduced in Fortino et al. [12] as an alternative. However, several sensors can communicate at the same time using this technique. Hardware architecture was established for the same reason. In addition to the cloud-based architecture previously stated, it looks at various other BSN configurations Gravina et al. [15]. Despite technological developments in this field, many people continue to employ outmoded methods to harm or even violate the privacy of their victims. Those with nefarious motives could launch an assault. Readers can be given erroneous sensing data by an attacker that results in inaccurate diagnosis. As a result, the victim's treatment could be placed on hold or even put at risk.

Hackers may take private information with the intent of extorting money or other harm. It is critical that healthcare facilities employ privacy and security safeguards when implementing IoT for remote health monitoring. There must be a set of encryption and authentication protocols in place for anti-adversarial attacks to work. By prohibiting unauthorised access to critical information, the public interest will be safeguarded. In order to prevent the misuse of private medical information, privacy must be safeguarded Zhou et al. [53], Ali et al. [7], Mollera et al. [28] and Kim et al. [24].

A flurry of ideas for IoT integration has been floated previously. The problem is that many of them weren't made with healthcare in mind Simplicio et al. [38] and Ray et al. [34]. If these solutions are employed, healthcare applications Moosavi et al. [29], Yang et al. [48] may not be effectively protected. In Simplicio et al. [38], an IoT solution is described for establishing a session key between two parties. Authentication and session management were completely overlooked by the researchers. Ray et al. [34] outlines an RFID ownership transfer mechanism for Internet of Things (IoT) use. There must be a way for the RFID reader and tag to verify each other's identities, but this has nothing to do with medical care. It has been decided to use IoT to improve mobility healthcare. The implementation of challenge response systems also made advantage of mobile sensors and users. Encryption was, on the other hand, a topic that had very little information available about it. In Yang et al. [48], a framework for an IoT-enabled integrated healthcare unit is proposed. Body sensors, servers, and data senders and receivers are not covered by their protocol, but users and servers are.

A BAN based architecture should include the victim, medical reader, medical server, and other stakeholders, according to him and others. This approach has a security issue that has been uncovered. The protocol appears to contain body sensors and wireless hubs, although it appears to be lacking in detail. Encrypted connections between medical readers and the wireless hub are ignored. In the world of wearables and biometric sensors, there is no way to verify each other's identities. A compelling setting is used to provide a foundation for remote victim observation in this study, which addresses these issues. There are no compromises in terms of data security or individual privacy in the proposed framework. This paper presents a novel method for secure end to end communications in a remote victim observation IoT application. A complete system model is given before a security technique is recommended. This study's findings can now be used by researchers and healthcare providers to develop remote victim observation systems.

For privacy concerns, mutual authentication, data integrity, user untraceability, and the absence of replay attacks must be met by the suggested approach. Secrecy must be maintained in both directions in order to meet industry standards. Authentication is the method by which a recipient determines whether or not the sender is genuine. Both parties will be able to use mutual authentication. It's crucial in a BAN. Senders and receivers must be able to verify each other's identities Yao et al. [49]. Without encryption, data on a network can be intercepted and used against the sender. It is possible to alter this type of data. It is also necessary to consider the data's integrity. The sender's message appears to have been misconstrued in this case. Because of this, it's necessary to create data transmission protocols that prevent against manipulation and maintain data integrity throughout the network.

Users' true physical locations are hidden from each other when connected to a network. Using the data sent by an assault, it is possible to pinpoint a person's physical position. Chen et al. [19] This is a security concern that BANs must deal with. Data can be intercepted if it is transmitted across a network that does not have adequate authentication or permission. A repeat performance by these fraudsters could lead to the theft of sensitive information. A recurrence is an example of this type of attack. Avoiding this type of attack is a security concern. It's possible to hack the session key during a session between two BAN participants. That's because they can speak with the victim using their session key at any time. This should be avoided in BAN to preserve the security of communications. With the help of reverse and forward secrecy Chen et al. [20], this can be achieved. A more secure internet of things is our goal with this paper's proposed study. Our contributions to the organisation can be seen in the following list of achievements.

1. We have created a mechanism for securely delivering data while protecting the privacy of the recipient in IoT use cases like remote victim observation (RVO).
2. Body sensors, data servers, receivers, and transmitters are just some of the many components that go into creating a system model. The RVO case study appears to have the support of all of these individuals and organisations.
3. In order to monitor a victim's vital signs (such as blood pressure and heart rate), a smartphone app has been developed for the victim, the doctor, and the victim's close family member.
4. A server side capability is being created to save, analyse, and make available to users on demand victim health data.
5. It is necessary to test RVO to check if it fits the aforementioned security requirements after implementing the recommended security strategy.

In the second section of the study, we conduct a literature review on IoT use cases such remote victim observation to assess their security. Section 3 contains research on safe IoT applications with an RVO (Motivational Scenario). Using the inspiring case in Section 3 as a backdrop, the implementation in Section 4 goes further. Stakeholders and the various stages of the proposed plan are detailed in Section 5. The planned course of action is considered in this section. Section 7 concludes with recommendations for future research.

2 Related work

There have been significant advances in remote victim observation research, as outlined in this section. According to Yew et al. [50], a real-time monitoring system for victims was proposed. After analysing an ECG from a cardiac victim, the monitoring findings were published online or via an app. Message Queuing Telemetry Transport (MQTT) was used to disseminate their information. Better still, jitter and noise signals would be decreased or eliminated entirely. Healthcare and patient monitoring architecture was described by Akkaset et al. [6]. An IoT-based WBAN-based system was created to monitor victims oxygen saturation and pulse rate. An in-depth case study was utilised to gauge the system's overall performance. In terms of data transmission, energy consumption, and general stability, it was shown to be more efficient than the current system. Shanin et al. [37] used the Internet of Things (IoT) to construct an e-Health record system that enables for remote victim surveillance. All of their vitals were being tracked by the device, including their pulse, temperature, and heart rate. In order to authenticate the identity of an individual, RFID can be employed. Maintaining a close eye on victims while also allowing for secure contact is critical to their well-being. Saha et al. [35] claims to have created IoT based health monitoring system Hassanalieragh et al. [17]. To make use of the sensors, a sensor network that was interconnected with the internet was created. Using a smartphone app, the vital signs of a victim can now be tracked in real-time.

A group led by Hassanalieragh et al. [17] and Mohammed Imtyaz Ahmed et al. [5] examined the challenges and opportunities presented by the Internet of Things in healthcare. Several layers of commonality were found in remote health monitoring, they found. Data gathering and transmission, cloud computing, and data storage are all examples of this. Researchers observed that remote health monitoring systems can be enhanced. A cloud based system called fog computing was employed by Rais et al. [33] to monitor remote victims. Fog aided offloading lowered power consumption while improving device performance. For real time victim monitoring, Uddin et al. [42] and his colleagues used the Internet of Things and it's numerous layers. Using these instruments, temperature, ECG, and humidity may all be monitored. Abawajy and Hassan et al. [1], pioneered Pervasive Patient Health Monitoring (PPHM). This thorough architecture for remote health monitoring includes an analysis of the scheme's energy efficiency and scalability.

The rising usage of sensors and IoT networks in the real world has opened the door for remote victim observation, according to Gomez et al. [13]. Users, clients, and servers all have a role in the system's structure. Both the victim and the doctor can use the system simultaneously. Three devices are linked to the system. This internet based system includes an ECG Glucometer, a sound device, and other components. By Wan et al. [43], an proposed a system known as Wearable IoT cloud-based health monitoring system was presented for real time health monitoring (WISE). Based on a body area sensor network (BASN), WISE is a wearable integrated sensor system. Rahman et al. [32] presented an RFID-based privacy preserving paradigm for healthcare systems Gope et al. [14]. The authors provided a variety of authentication and access control measures. The authors have offered many models for achieving privacy in IoT applications. They evaluated RFID to near field communication (NFC) and decided to go with RFID because of its distance, the advantages of Internet of Things (IoT) integration in healthcare, as well as privacy and security are highlighted. Due to the lack of cloud aided effective security measures as disadvantages, using an Internet of Things connected RFID-based information system, it is possible to keep track of the health status of victims. Security measures are in place to protect healthcare-related information. For example, they discovered ways to improve the overall quality of the healthcare system while protecting victims privacy by using an RFID-based technology.

Gope et al. [14]. presented RFID-based privacy preserving authentication for scattered IoT application cases. For the final step in the authentication procedure, we turned to the hash function. An authentication mechanism is used in conjunction with RFID network clustering to develop this system. As a result, it can protect against phishing and malware attacks. It was designed by Wu et al. [45] for medical applications to use an RFID based anonymous authentication method. An RFID system based on a hash algorithm served as the foundation for the system. Christos et al. [40] A 6G mobile network and smart buildings are all part of Stergiou and his colleagues security architecture. Technology such as edge and cloud computing are used to achieve its goals. Blockchain technology is employed by Espisito et al. [10] when it comes to the administration of distributed identification and authorisation components. Finally, the FIWARE platform can be used to access the data. According to Tewari and Gupta et al. [41], cross-layer and IoT security issues can be compared to traditional security issues. Four-image encryption was created using the computer generated hologram, chaos, and

Quaternion Fresnel Yu et al. [51] transformations, according to Yu and colleagues. In order to detect COVID-19 using deep learning, Sedik et al. [36] advocated using LSTM and Convolutional Neural Networks (CNN). Adat and Gupta et al. [3] studied the security of IoT devices Pu and Li et al. [31] suggested a lightweight authentication method based on a hybrid approach in order to combine a chaotic system with a physically unclonable function. “Man in the Middle” attacks can be used to target unmanned aerial vehicles, according to Li and Pu et al. [26]. Using lightweight signatures, they devised a defence against the attack. Existing remote health monitoring systems employ a wide range of techniques, according to the research. RFID based authentication has been proved to improve IoT security. Remote victim observation in an IoT integrated healthcare system will need a solution that is even more secure than WBAN.

3 Motivating scenario

Research shows that security and lightweight design with multiple IoT layers are critical. Reusable components in the system simplify the research process considerably. Testing the framework’s capabilities is done through prototype applications. An IoT enabled healthcare scenario is depicted in Fig. 1. As a result, learning more about it is a primary goal of this study. This is an example of “Remote Victim Observation (RVO)”.

Remote victim observation is therefore brought to light. In addition, the case study’s many participants must be able to communicate with each other in it to be successful. If this scenario is implemented without adequate security measures, victim information and communications

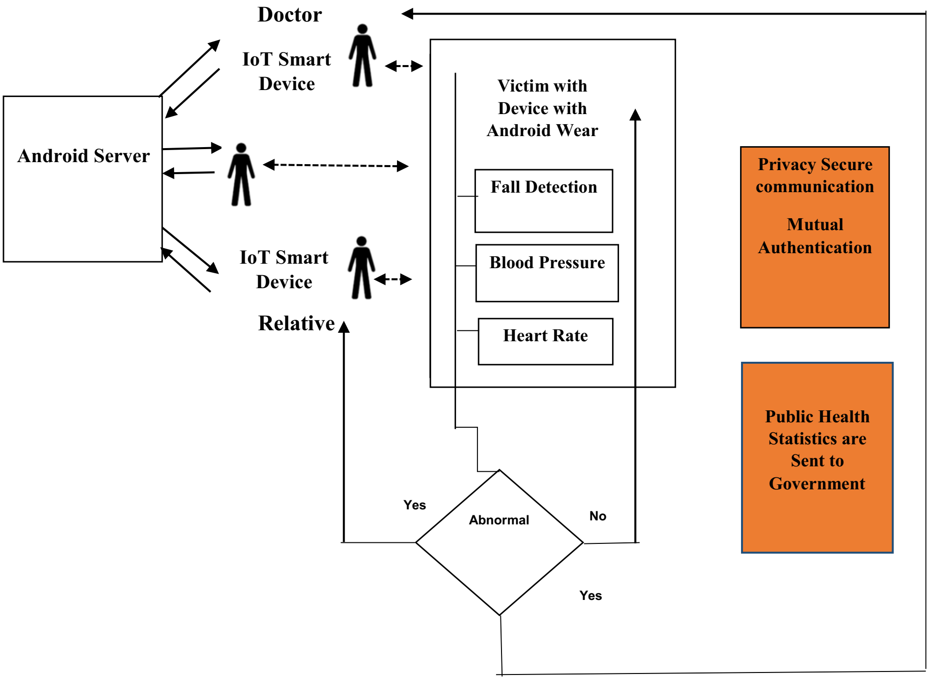

Fig. 1 Architecture of RVO and IoT procedure

could be put at danger. The sensitivity of healthcare data necessitates the use of a security architecture. Android wear OS is installed on all of the victim's wearable devices. This device can tell you whether a victim's vital signs are out of whack. Victims and their families are informed if any of the signs are not as they should be. The ability to monitor your heart rate, blood pressure, and even determine if you've fallen is now at your fingertips. The data is stored on an android server and accessed through the app. It is possible for a doctor or a victim's family member to view victim information via an android server. When developing a secure RFID authentication system, an end to end communication system, and privacy protection, the following scenario must be used as a motivating factor. This proposed scheme is controlled remote victim vital signs in abnormalities and protect the life of human with secure and privacy of their data to lead better quality of life and it is monitoring the patient data to respective doctors and relatives.

4 Implementation of motivating scenario

Temperature, blood pressure, heart rate and blood sugar levels can all be monitored remotely using devices that can provide real-time data on health indices like these. To do this, we intend to develop a system that comprises mobile services, server-side processing, and data collection (from sensors or from simulation). Everyone participating in the system—victims and caregivers alike—is connected to it in some way.

Assisting victims and the elderly with their data collection (sensors). When compared to more time consuming methods, the process of automatically detecting data from a victim is more efficient. Their medical records will be accessible to their primary care physicians and family members. Victims and their families will be alerted if sensors detect an abnormal health status among the elderly/infirm members of the community. Victims' basic conditions and precise whereabouts are verified before emergency assistance are dispatched. In addition, family doctors can access a variety of victim data through the device. To better comprehend a victim's or elderly person's medical status, doctors use medical history data. It is also possible to monitor and analyse certain disorders using this method. Health care policies and services can be tailored to meet the requirements of individuals and groups.

According to study, more than a third of all seniors who fall seek for assistance because they are either unresponsive or disoriented. We don't want to be in the same situation again. Family members of the elderly can also call emergency assistance.

Figure 2 depicts all of the RVO IoT use case's actions. A remote victim's fall, blood pressure, and heart rate can all be monitored using this device. Using wearable technology with a body sensor, you can keep an eye on these important metrics. It is feasible for a doctor and a victim's relative (Attendant) to access the victim's medical records via a mobile app. It is possible to look at sensor data, make an emergency call, and see the doctor's opinion. To evaluate if a victim's condition is normal, the system can analyse data.

According to Fig. 3, interactions between the victim, doctor, and relative all have a role in this condition. This smartphone software allows for simultaneous use by three persons. Before contacting a doctor or a relative, a victim can check health information and the doctor's opinions (Attendant). Apps can be used to maintain track of victims who have fallen and can no longer communicate with a medical expert. Once the victim has been correctly identified and is able to access the main activity, an interface for any eligible operations may be found. Your heart rate and blood pressure are critical medical measures. An HTTP request is made to

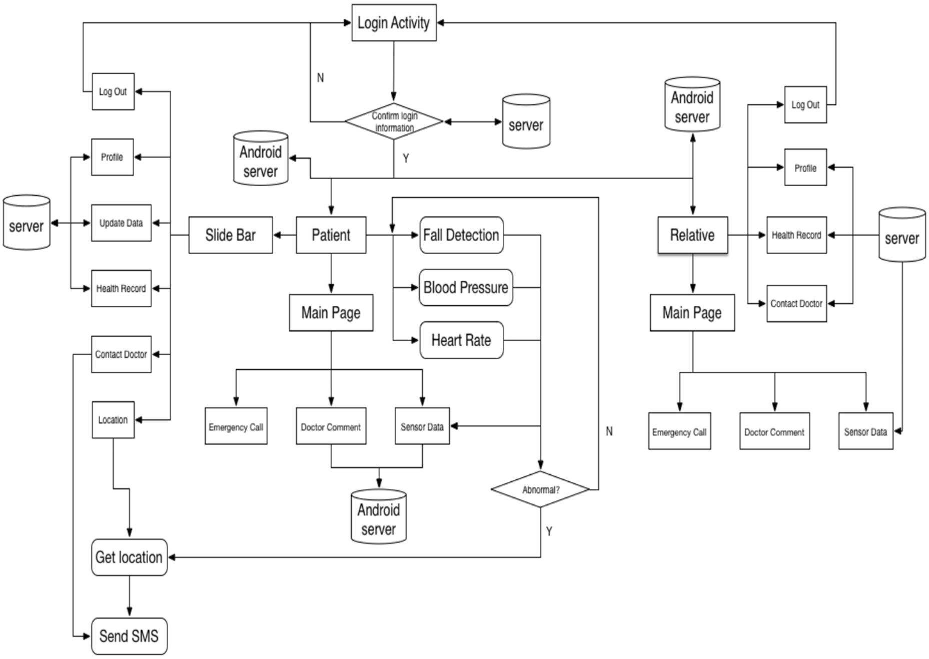

Fig. 2 Features of health data and from a remote victim

the server each time one of these options is selected. During an emergency, the victim can use the app to reach both the doctor and a close relative.

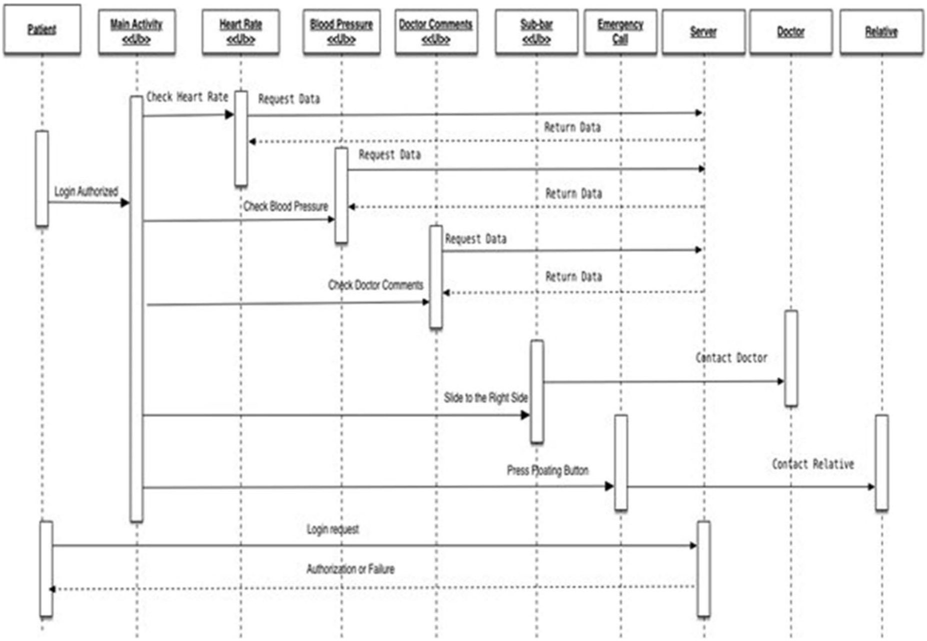

Fig. 3 Smartphone steps

RVO packages are used for server side features. The services it offers can be used for a wide range of purposes. Any number of functions can be performed by mobile apps, but the server is always in control. The server keeps track of data and establishes safe connections, as detailed in Section 7. The motivating scenario (RVO) aims to illustrate a comprehensive security architecture that enables secure, lightweight, and privacy preserving communication between all parties. As a result, the RVO integrated into the Internet of Things is extremely secure. Figure 4 shows a web based application for updating user profiles and contact information.

Several participants are depicted in Fig. 5 as part of the overall system. All items in an Internet of Things (IoT) environment must be uniquely identified. With their long range and absence of line of sight, RFID tags are a better option than barcodes for this application. To keep track of things in the Internet of Things, RFID tags are employed. To read the information stored on an RFID tag, you'll need an RFID reader. An RFID tag and a reader are included in the proposed system.

The suggested system is built on a number of design choices. The programme was divided into two parts a server component and a user facing component. In both mobile and web based applications, the backend is a component on the server. An abnormal occurrence might be displayed on the victim's mobile client application while information is saved on the server. The recommended method should be used and implemented in order to ensure secure remote victim observation. Real world healthcare applications can be employed using this technology. Remote victim observation is one example of how it can be put to use in the real world. In many nations, the lack of real time victim monitoring leads in a significant number of deaths.

5 Proposed scheme for RVO IoT use case

RVO's secure communications are covered in this section (Section 6).

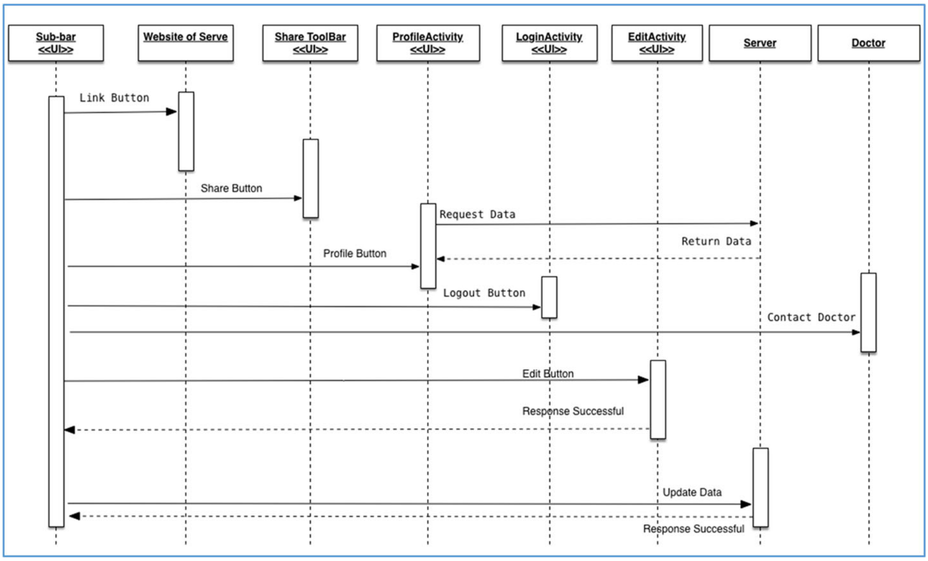

Fig. 4 Sequence server side functionality

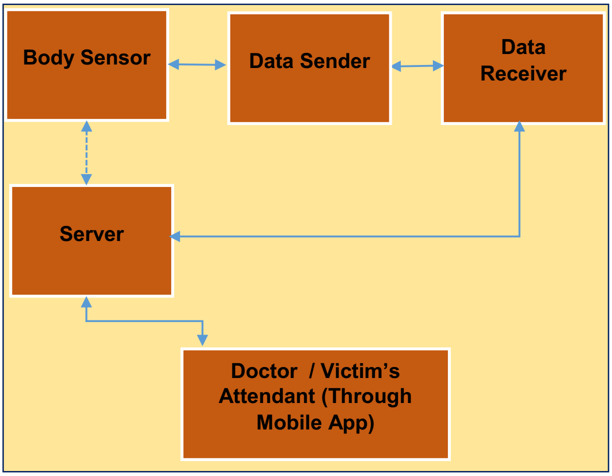

Fig. 5 Privacy and security overview

How the RVO IoT use case is implemented. Tracking health data, such as falls, blood pressure, and heart rate, from a remote victim is possible with this device. Wearable technology with a body sensor can keep tabs on these critical indicators. By using the smartphone app, both the victim's doctor and the person who is taking care of them can look over their medical records. Sensor data can be examined, emergency calls can be made, and the doctor's opinions can be viewed. For example, the system can analyse a victim's condition to determine if it is a normal or abnormal state.

The system's conceptualization.

Based on the example in Section 3, this diagram depicts the overall system design. Both a sender and a receiver for both the doctor and the victim, a mobile app will alert them when something is off with their health.

A battery powered circuit is used to monitor vital signs, such as blood pressure and heart rate, in victims. In addition to that, he's sporting a smartwatch.

Sensor data is transmitted to a distant server through Bluetooth.

The data sent to this receiver is evaluated by this receiver. For this operation, a smartphone app will be used by both the doctor and the victim.

The data is stored on a server and analysed by a computer programme. Data exchanges must be documented for security reasons. Figure 5 depicts a rough sketch of the design.

Based on a system architectural concept, we have created this diagram to show the many parties involved in communication. Confidentiality and safety are ensured by a few simple steps. See Fig. 5 for an overall view of how things will go.

1. Both the sender and the recipient must have a channel account. However, it's a safe bet. It's necessary to know who sent the message and who it was intended for. The unique identifier (UUID) is the name given to the identifier (UUID). System parameters are computed on the server using elliptic curve groups. The a & b curve parameters, the G generator point, the ord (G), and the cofactor are employed (h). Secure and lighter.

2. All data senders and body sensors must be registered B. A. The data sender and body sensor safely transfer identifiers to the data receiver. The data receiver returns polynomial parameters.
3. A data transmitter collects data from a body sensor after successful authentication has been accomplished. Data that has been encrypted is fed into the system.
4. By supplying the recipient with information, the sender validates the recipient's identity. It is defined by its elliptic curve group (ECG) and it's unique identifier (ID). The sender sends the recipient's encrypted health information after they have both authenticated each other.

An initialization, registration (using a transmitter and receiver), authentication and communication are the three stages of the suggested technique. Table 1 depicts the system's identifiers.

5.1 Initialization phase for the system

During the initialization step, the server computes required parameters and sends public parameters to the data sender and data receiver.

The steps that make up the initialization procedure are described below.

1. The steps that make up the initialization procedure are described below. A tuple of elliptic curve groups labeled (Fp, E/Fp, G, P) and a k-bit prime marked as p are considered by the server.

Table 1 Notations

Notation	Description
CHK_x	x' s verified message
$D_x(m)$	Message m is decrypted using session key x.
E/F_q	An elliptic curve E over Fq
$E_x(m)$	Message m is encrypted using session key x.
F_q	A prime finite field
H_iO	ith one-way hash function
ID_{HS}	Body sensor id
ID_{MR}	Medical reader id
ID_{PR}	The personal reader id
ID_x	Denotes a random number. Elliptic curve group uses it.
K_i	Denotes a polynomial function of information related to elliptic curve.
S_x	Signature of elliptic curve group of x.
c_i	The session key and transaction number encrypted sensing data
$Data$	Data sensed by body sensor.
$f(x,y)$	Denotes f(x, y) equal to f(y, x) as polynomial function.
G	Denotes cyclic additive group with composite order q
hO	A one-way hash function
P	The group G's generator
PEK	It is the session key established between two parties namely data receiver and data sender
PK	Denotes a public key which is in the system PK=sP
Q	Denotes a k-bit prime
r, a, b	Random numbers
S	A secret key of the system
$T\ ID$	Denotes a transaction ID
$A \overset{?}{=} \mathrm{B}$	Checks whether A and B are equal

2. A tuple of elliptic curve groups labeled (Fp, E/Fp, G, P) and a k-bit prime marked as p are considered by the server. As demonstrated in Eq. 1, the server also computes a public key using a secret key represented by s.

$$PK = s^{P} \tag{1}$$

3. After that, the server chooses a hash function (H1(), H2(), H3(), H4()) to distribute to all data senders and receivers (Fp, E/Ep, G, P, PK, H1(), H2(), H3(), H4()).

5.2 Registration of body sensors

The body sensor must be registered by the data receiver. The steps are as follows:

1. The body sensor selects and sends to the receiver a Universally Unique ID (UUID) specified as IDHS.
2. The data receiver then computes the polynomial f (x, y) and sends it to the body sensor as (HPHS, SID).

The computations are the same as in Eqs. 2 and 3. SID stands for sensor identification number. C1 denotes the session key and transaction number encrypted sensing data.

$$HP_{HS} = f\ (ID_{HS}, y) \tag{2}$$

$$C1 = h\ (SID) \tag{3}$$

3. The body sensor receives the same (HPHS, SID) and stores it in memory.

5.3 Data sender registration

It is necessary to register the data sender, as well as the data receiver and server. The steps are as follows:

1. An IDPR is chosen as a Universally Unique ID (UUID) by the data transmitter and sent to the receiver.

The data receiver then computes and communicates the polynomial f (x, y) to the data sender (HPPR, SID). The calculations in Eqs. 4 and 5 are the same. SID stands for sensor identification number. C2 denotes the session key and transaction number encrypted sensing data.

$$HP_{PR} = f\ (ID_{PR}, y) \tag{4}$$

$$C2 = h\ (SID) \tag{5}$$

2. The body sensor receives the same (HPHS, SID) and stores it in memory.
3. The data sender chooses and sends an IDPR identity to the server.
4. Before delivering (RPR, SPR) to the data reader, the server chooses a random number r and computes (Eqs. 6, 7, and 8), P denotes the group G's generator.

$$R_{PR} = rP \tag{6}$$

$$h_{PR} = H_1\left(ID_{PR} \| R_{PR}\right) \tag{7}$$

$$S_{PR} = r + h_{PR}S \tag{8}$$

5. After that, the data reader does the Eq. 9 verification. After successful verification, that (RPR, SPR) will be saved in the personal reader's memory.

$$S_{PR}P = R_{PR} + H_1\left(ID_{PR} \parallel R_{PR}\right) PK \tag{9}$$

5.4 Data receiver registration

The server's database should be updated to include the data recipient. Direct mutual authentication between the data transmitter and receiver is possible. The server registration for the data recipient is as follows. The data receiver received the victim data and it can be process to the server, it communicates to victim attendant and doctor through the mobile app to protect the life of the victim.

1. The data receiver selects and sends an IDMR identity to the server.

2. The server then performs the computations in Eqs. 10, 11, and 12 with a random number r before delivering (RMR, SMR) to the data receiver.

$$R_{MR} = rP \tag{10}$$

$$h_{MR} = H_1\left(ID_{MR} \parallel R_{\mathrm{MR}}\right) \tag{11}$$

$$S_{MR} = r + h_{MR}S \tag{12}$$

3. When the data recipient receives it, Eq. 13 is used to confirm it. If the verification is successful, the data is saved in the memory of the data receiver.

$$S_{MR}P = R_{MR} + H_1\left(ID_{MR} \parallel R_{MR}\right) PK \tag{13}$$

5.5 Authentication and communication

The data reader must connect to the data receiver in order to send data or use any other service. As a result, mutual authentication is essential between the two parties. The steps for authentication and communication are as follows.

The data transmitter computes (Eq. 14) and sends (IDPR, c) to the body sensor when it requires victim health data from the body sensor. C3 denotes the session key and transaction number encrypted sensing data.

$$C3 = h\ (SID) \tag{14}$$

1. It is verified by the body sensor. The body sensor executes the calculations in Eqs. 15, 16, and 17 after successful verification and sends (IDHS, d, e) to the data sender.

$$K_{HP} = f\ (ID_{HS}, ID_{PR}) \tag{15}$$

$$d = E_{KHP}\ (data) \tag{16}$$

$$e = h\left(data \parallel K_{HP}\right) \tag{17}$$

2. The data sender computes and verifies the information (as in Eqs. 18 and 19). After successful verification, the data sender provides health data to the data receiver.

$$K_{HP} = f\ (ID_{PR}, ID_{HS}) \tag{18}$$

$$data = D_{KHP}\ (d) \tag{19}$$

3. The data sender then chooses a random number a, calculates (as in Eq. 20), and sends to the data receiver (IDPR, RPR, TPR).

$$T_{PR} = aP \tag{20}$$

4. In Eqs. 21, 22, 23, 24, and 25, the data receiver uses a random number b to determine the session key.

$$T_{MR} = bP \tag{21}$$

$$PK_{PR} = R_{PR} + H_1\Big(ID_{PR}||R_{PR})PK \tag{22}$$

$$K_{MP1} = S_{MR}T_{PR} + bPK_{PR} \tag{23}$$

$$K_{MP2} = bT_{PR} \tag{24}$$

$$PEK = H_2\left(K_{MP1} \parallel K_{MP2}\right) \tag{25}$$

5. The data receiver then chooses a transaction id (TID), computes (as in Eqs. 26, 27), and transmits the data (ID_{MR}, R_{MR}, T_{MR}, g, CHK_{PM})

$$g = E_{PEX}\ (TID) \tag{26}$$

$$CHK_{PM} = H_3\left(PEK\ \| T_{PR}\right) \tag{27}$$

6. Using Eqs. 28, 29, 30, and 31, the data sender computes and verifies the session key.

$$PK_{MR} = R_{MR} + H_1\left(ID_{MR}\ \|\ \ R_{MR}\right)\ PK \tag{28}$$

$$K_{PM1} = S_{PR}T_{MR} + aPK_{MR} \tag{29}$$

$$K_{PM2} = aT_{MR} \tag{30}$$

$$PEK = H_2\ \left(K_{PM1}\ \| K_{PM2}\right) \tag{31}$$

7. After successful verification, the data sender confirms the legality of the data receiver. It does so by computing Eqs. 32, 33, 34, and 35 and transmitting them to the data receivers as (ID_{PR}, CHK_{MP}, ci)

$$TID = D_{PSK}\ (C) \tag{32}$$

$$c_i = E\ \left(PEK\ ||TID\right)^{(data)} \tag{33}$$

$$CHK_{MP} = H_3\ \left(PEK\ \| T_{MR}\ \| TID\right) \tag{34}$$

$$TID_{new} = H_4\,(TID) \tag{35}$$

8. The data receiver then performs a $\mathrm{CHK_{MP}}$ check.

9. After successful verification, the session between the two parties is successfully constructed. Once the session key is established, the data receiver computes data and changes the transaction number (as in Eqs. 36 and 37, respectively) for further communication.

$$data = D_{\left(PEK\,\|TID\right)}\,(C_i) \tag{36}$$

$$TID_{new} = H_4\,(TID) \tag{37}$$

6 Security evaluation

Using the motivating case depicted in Fig. 1, as well as the system model depicted in Fig. 5, Section 5's method is evaluated. Everything from processing and transmission costs to replay attack protection and user untraceability is thoroughly scrutinised.

6.1 Mutual authentication

The sender and recipient are both confirmed to be who they say they are. To complete the process, a new session key is generated. By deploying an unlicensed data receiver, the proposed solution prevents an adversary from gaining access to sensitive victim health information. The attacker is doomed to fail because the illicit data recipient is not registered. A precise calculation of the session key is impossible. This means that the attacker will be unable to identify the true sender of the compromised data. An attacker also cannot make advantage of unauthorised data transmitters. An unregistered reader has access to sensitive material, but the recipient or server is ignorant of it. Mutual authentication protects IoT based healthcare against these threats.

6.2 Privacy of users

A person's current location can be obtained as part of several privacy attacks. Since location data is extremely private, avoid this at all costs. Known as "User untraceability," this is what we mean. A few examples: The recipient's or sender's location. One of the alternatives for data readers is CHKMP. It is chosen at random for each communication round in order to thwart attempts to trace it's location. This method protects both your identity and your whereabouts.

6.3 Data integrity

Another aspect of IoT security to consider is the integrity of the data. ECC is a mechanism for encrypting data and creating session keys that is available for purchase. Signatures such as kpm1-kpm2 and kpm3-kpm3 cannot be used by an adversary to produce session keys (KMP1, KMP2). Only by creating a successful session key can proper communication be achieved. When a data receiver sends an email to a hostile attacker, for example, the email may be intercepted and forwarded. The ability of legitimate data senders to check the integrity of their own data thwarts attacks. It's also impossible for an intruder to crack the session key. The lawful data sender has the ability to authenticate incoming communications, therefore any data integrity attack will be thwarted by this capability. As a result, any opponents who try to change the subject will be doomed to a defeat.

6.4 Reverse confidentiality

Data integrity and communication between sender and receiver are ensured by the session key. Even if an attacker gains access to such a session, the proposed technique ensures forward and backward confidentiality. Because the session is generated randomly, the attacker cannot utilize the compromised session key to attack. The current round will fail if the attacker uses a compromised session key. As a result, the method can manage both forward and reverse secrecy.

6.5 Preventing replay attacks

Messages are sent and received in the RVO IoT application use case. These communications may be intercepted by attackers. To transmit identical communications to the target data sender or receiver, attackers can mimic a legal data sender or recipient. Security is enhanced by changing the message for each round. The proposed method does not allow for replay attacks because the same message cannot be sent repeatedly. Because the messages are continually changing, a replay assault is guaranteed to fail.

6.6 Accessibility

According to our findings, the IoT RVO application possesses a secure security technique. Keeping the system safe while enabling the desired functionality is doable. The dependability of the hardware has not been verified. RVO, on the other hand, has been thoroughly tested and found to be dependable. Because cloud services are always available, regardless of time or location, your system's availability is increased when you use the cloud.

6.7 Fee for computing

For the strategy's computing expenses, see Table 2. data transfer, authentication, and communication are all considered while registering body sensors. When determining the final decision, all parties involved are considered. Sensors and other input/output devices are included.

There are a variety of symbols used to indicate the cost of calculation in the table the computational cost of symmetric encryption is abbreviated (TEnc). According to the (TCmp)

Table 2 Computed cost of comparison

Phase | Party	Server	Data receiver	Data sender	Body sensor
Registration of body sensor	N/A	$1T_P+1T_H$	N/A	N/A
Registration of data sender	$2T_{Mul}+1T_H$	$1T_P+1T_H$	$2T_{\mathrm{Mul}}+1T_H+1T_{\mathrm{Cmp}}$	N/A
Registration of data receiver	$2T_{\mathrm{Mul}}+1T_H$	$2T_{\mathrm{Mul}}+1T_H+1T_{\mathrm{Cmp}}$	N/A	N/A
Authentication & communication	N/A	$5T_{\mathrm{Mul}}+1T_H+1T_{\mathrm{Cmp}}$	$1T_P+5T_{\mathrm{Mul}}+7T_H+2T_{\mathrm{Cmp}}+3T_{\mathrm{ENC}}$	$5T_P+2T_H+1T_{\mathrm{Cmp}}1T_{\mathrm{ENC}}$

abbreviation, "computed cost of comparison" is "computed cost of comparison." How long does it take to solve the hash function. The cost of multiplying two numbers is referred to as (TMul). TH is the price associated with computing a polynomial function. For body sensor registration, a polynomial function and a hash function are required. Data transmitter registration necessitates two multiplications and a hash function; receiver registration necessitates a polynomial and a hash function. A hash function, two multiplications, and a comparison are required by the server to register data receivers, whereas the receiver only needs one. Time consuming components of computing are authentication and communication. To conduct the data receiver's symmetric encryption and comparison, the data sender must perform five multiplications and one polynomial operation as well as seven hash functions; the body sensor must perform two comparisons.

Using Table 3, we can see how much the scheme's communication expenses have changed over time. Message length, number of cycles, and time all factor into the available bandwidth, which ranges from 14 Mpbs to 100 Mbps at various phases of processing.

Testing of the proposed strategy's communication abilities. A 256-bit AES key is assumed to be required for messages like random number, pid, and id, as is a hash key of 160 bits and an elliptic curve modular key of 160 bits. The length of the message and the number of rounds have an impact on the overall time. 3G and 4G networks operate at different speeds. The greatest cycles are consumed during authentication and communication. Only 0.024 milliseconds are required at 4G speeds. It takes five rounds and 0.175% of a second to complete the test with 3G speeds.

6.8 Feature analysis

Then he and others Chen et al. [21] Many features of the system should be compared, including the capacity to prevent replay attacks, anonymity of users, and forward and backward secrecy. The following are the comparison's specifics: Item #4 (Table 4).

Table 3 Communication cost analysis

Phase/Item	Length of message	Number of rounds	14 Mbps Speed (3G)	100 Mbps Speed (4G)
Registration of body sensor	400 bits	2	0.029 ms	0.004 ms
Registration of data sender	880 bits	4	0.063 ms	0.009 ms
Registration of data receiver	480 bits	2	0.034 ms	0.005 ms
Authentication & communication	2448 bits	5	0.175 ms	0.024 ms

Table 4 Features compared with He et al.'s Scheme (Y for Yes, N for N)

Feature/Scheme	Scheme of He et al. [18]	Proposed Scheme
Comprehensive Scheme	N	Y
Forward and Backward Secrecy	N	Y
Replay Attack Prevention	Y	Y
User Untraceability	Y	Y
Data Integrity	Y	Y
Mutual Authentication	N	Y

A complete method to safeguard the privacy of numerous parties has been presented for healthcare apps linked to the internet of things. He and his colleagues' technique lack features like forward and reverse secrecy, but this one has. The He et al. approach lacks mutual authentication. Data integrity, user anonymity, and replay protection are all included in both systems, as well. The proposed method can be used in IoT use cases such as "Remote Victim Observation" to provide greater security and privacy for communications.

6.9 Information leakage and privacy comparison

Consequently, privacy is a crucial problem in this investigation. To measure privacy, the value ranges from 0.0 to 1 (R denote privacy as a function of the number), with 1 being the most secure and 0.0 the least secure. There are a staggering number of tags that have been hacked when it comes to privacy. Tags are counted by the letter N. A system's integrity depends on every tag in it. The amount of personal information that has been compromised is measured by the number of tags that have been compromised Nohl et al. [30].

Table 5 shows the level of privacy for each method as well as the number of compromised nodes.

Table 5 Level of privacy vs. number of compromised tags

No. of compromised tags (C)	Level of privacy (R)		
	PriSens [32]	Group based authentication [8]	Proposed
0	0.995	1	1
10	0.745	0.75	0.75
20	0.545	0.55	0.55
30	0.393	0.398	0.4
40	0.28355	0.28855	0.29
50	0.2139	0.2189	0.22
60	0.14425	0.14925	0.15
70	0.1144	0.1194	0.12
80	0.10445	0.10945	0.11
90	0.0945	0.0995	0.1
100	0.791	0.796	0.8
110	0.04475	0.04975	0.05
120	0.04475	0.04975	0.05
130	0.0348	0.0398	0.04
140	0.02485	0.02985	0.03
150	0.02485	0.02985	0.03
160	0.0149	0.0199	0.02

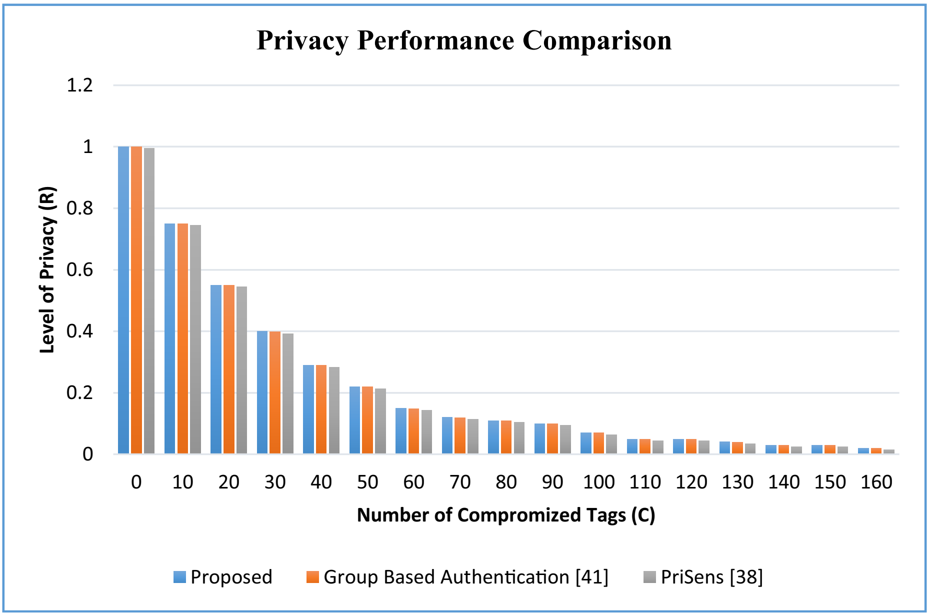

Fig. 6 Level of privacy comparison

How many tags have been hacked and how much privacy they have is illustrated in Fig. 6. The number of tags is represented by the horizontal axis, while the level of privacy is represented by the vertical axis. It is more likely that a tag will be hacked if it is more private. Researchers observed that the proposed approach provides a higher level of privacy than currently available for a wide variety of compromised tags. As a result of this approach, a higher level of privacy can be observed.

Table 6 Information leakage vs. number of compromised tags

No. of compromised tags (C)	Information leakage (bits)		
	Proposed	Group based authentication [8]	PriSens [32]
0	0	0	0
10	0.95	1.5	1
20	1.9	3	2
30	2.85	4.5	3
40	3.325	5.25	3.5
50	3.61	5.7	3.8
60	3.895	6.15	4.1
70	4.18	6.6	4.4
80	4.465	7.05	4.7
90	4.75	7.5	5
100	5.035	7.95	5.3
110	5.32	8.4	5.6
120	5.605	8.85	5.9
130	5.89	9.3	6.2
140	6.175	9.75	6.5
150	6.46	10.2	6.8
160	6.745	10.65	7.1

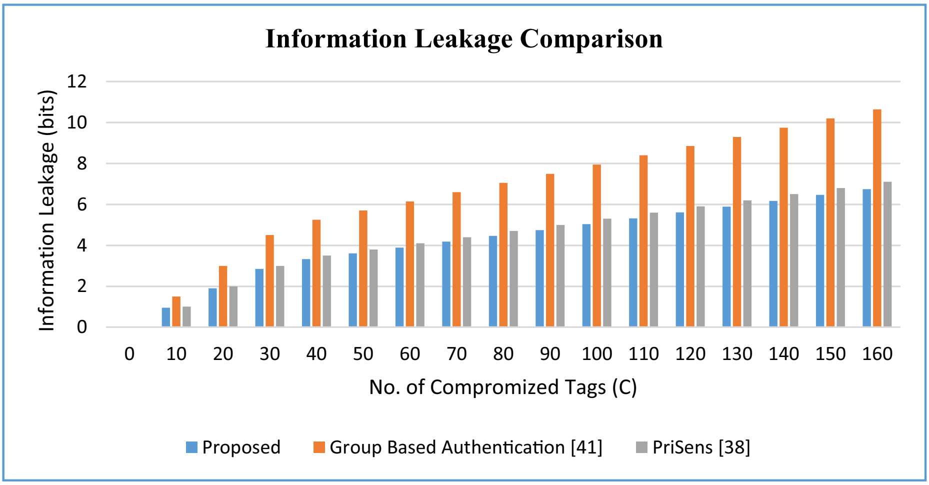

Fig. 7 Information leakage against number of compromised tags

Table 6 shows how information leakage is measured against the number of compromised nodes for each strategy.

Figure 7 shows the number of compromised tags in proportion to the amount of information that has been released. It is shown on the horizontal and vertical axes: the number of compromised tags and the amount of data leaked in bits. Data leakage is being exacerbated by an increase in the number of compromised tags. Because of the lesser number of vulnerable nodes, the proposed solution had a lower impact on information leakage. Data leaking can be prevented more effectively with the proposed solution than with current solutions.

7 Conclusion and future work

Item to item communication has become easier because to recent technology advancements (physical and digital). When it comes to connecting physical and digital devices, the Internet of Things (IoT) and radio frequency identification (RFID) have made this ideal come true. Fog computing, mobile cloud computing, and cloud computing can all be used in IoT applications. Connecting billions of devices and items is possible with the Internet of Things (IoT). It has had a substantial (positive) impact on a wide number of industries around the world. The Internet of Things is revolutionising healthcare by allowing victims to monitor their own health remotely, which improves both their quality of life and the quality of care they receive. As a result of the large range of devices, protocols, and standards used in IoT applications, these applications are open to numerous dangers. Concerns about the security of Internet of Things (IoT) applications require additional investigation. "Remote Victim Observation" use case for Internet of Things will be studied empirically as a consequence. When building an effective model, keep in mind that it's made up of a number of parts that connect in a way that's both safe and private. All of the critical security factors were handled in our plan of action. This solution protects users from being traced and prevents replay assaults. Secrecy is maintained both in the present and in the past. In the IoT case study, this technique was compared to He et alis. and found to have higher communication security capabilities than those of the latter. This system's ultimate goal is to become a wireless body area network (WBAN) that integrates IoT and has a significant impact on the medical industry.

Code availability N/A

Data availability N/A

Declarations

Research involving human participants and/or animals This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent No studies with human participants or animals are involved in this article.

Ethics approval N/A

Consent to participate N/A

Consent for publication N/A

Conflict of interest/Competing interest Authors declare that there are no conflicts of interest/competing among themselves

References

1. Abawajy JH, Hassan MM (2017) Federated internet of things and cloud computing pervasive patient health monitoring system. IEEE Commun Mag 55(1):48–53
2. Abbas A, Khan S (2014) A review on the state-of-the-art privacy preserving approaches in e-health clouds. IEEE J Biomed Health Inform 18:1431–1441
3. Adat V, Gupta BB (2017) Security in internet of things: issues, challenges, taxonomy, and architecture. Telecommun Syst 67(3):423–441
4. Ahmed I, Kannan G (2018) A review on present state-of-the-art on internet of things. J Adv Res Dyn Control Syst:352–358
5. Ahmed MI, Kannan G (2020) Overcoming privacy and security challenges of internet of things applications. Int J Future Gener Commun Netw 13(1):1550–1556
6. Akkaş MA, Sokullu R, ErtürkÇetin H (2020) Healthcare and Patient Monitoring Using IoT. Internet Things 11:1–12
7. Ali A, Irum S, Kausar F, Khan F (2013) A cluster-based key agreement scheme using keyed hashing for body area networks. Multimedia Tools Appl 66:201–214
8. Avoine G, Buttyan L, Holczer T, Vajda I (2007) Group-based private authentication. In: Proc. of WoWMoM, pp 1–6
9. Chiuchisan I, Dimian M Internet of things for e-Health: an approach to medical applications. In: Proceedings of the IEEE international workshop on computational intelligence for multimedia understanding (IWCIM), Prague, Czech Republic, 29–30 October 2015, pp 1–5 Sensors 2017, 17, 2919 18 of 18
10. Esposito C, Ficco M, Gupta BB (2021) Blockchain-based authentication and authorization for smart city applications. Inf Process Manag 58(2)
11. Fortino G, Parisi D, Pirrone V, Fatta GD (2014) BodyCloud: a SaaS approach for community body sensor networks. Future Gener Comput Syst 35:62–79
12. Fortino G, Galzarano S, Gravina R, Li W (2015) A framework for collaborative computing and multi-sensor data fusion in body sensor networks. Inf Fusion 22:50–70
13. Gómez J, Oviedo B, Zhuma E (2016) Patient monitoring system based on internet of things. Proc Comput Sci 83:90–97

14. Gope P, Amin R, Hafizul Islam SK, Kumar N, Bhalla VK (2018) Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Futur Gener Comput Syst 83:629–637
15. Gravina R, Alinia P, Ghasemzadeh H, Fortino G (2017) Multi-sensor fusion in body sensor networks: state-of-the-art and research challenges. Inf Fusion 35:68–80
16. Han J, Susilo W, Mu Y (2015) Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE Trans Inf Forensics Secur 10:665–678
17. Hassanalieragh M, Page A, Soyata T, Sharma G, Aktas M, Mateos G, … Andreescu S (2015) Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: opportunities and challenges. In: 2015 IEEE international conference on services computing, pp 1–8
18. He D, Chen C, Chan S, Bu J (2012) SDRP: a secure and distributed reprogramming protocol for wireless sensor networks. IEEE Trans Ind Electron 59:4155–4163
19. He D, Chen C, Chan S, Bu J, Vasilakos A (2012) A distributed trust evaluation model and its application scenarios for medical sensor networks. IEEE Trans Inf Technol Biomed 16:1164–1175
20. He D, Chen C, Chan S, Bu J, Vasilakos A (2012) ReTrust: Attackresistant and lightweight trust management for medical sensor networks. IEEE Trans Inf Technol Biomed 16:623–632
21. He D, Chen C, Chan S, Bu J, Zhang P (2013) Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE J Biomed Health Inform 17:664–674
22. Kannan G, Thameez RM (2015) Design and implementation of smart sensor interface for herbal monitoring in IoT environment. Int J Eng Res:469–475
23. Khemissa H, Tandjaoui D A lightweight authentication scheme for E-Health applications in the context of internet of things. In: Proceedings of the international conference on next generation mobile applications, services and technologies, Cambridge, UK, 9–11 September 2015, pp 90–95
24. Kim H, Kim CH, Chung JM (2012) A novel elliptical curve ID cryptography protocol for multi-hop ZigBee sensor networks. Wirel Commun Mob Comput 12:145–157
25. Lee J, Kapitanova K, Son S (2010) The price of security in wireless sensor networks. Comput Netw Int J Comput Telecommun Netw 54:2967–2978
26. Li Y, Pu C (2020) Lightweight digital signature solution to defend micro aerial vehicles against Man-In-The-Middle Attack. In: 2020 IEEE 23rd international conference on computational science and engineering (CSE), pp 92–97
27. Liang K, Susilo W (2015) Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans Inf Forensics Secur. 10:1981–1992
28. Mollera S, Newe T, Lochmann S (2012) Prototype of a secure wireless patient monitoring system for the medical community. Sens Actuators A Phys 173:55–65
29. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, Isoaho J (2016) End-to-end security scheme for mobility enabled healthcare internet of things. Future Gener Comput Syst 64:108–124
30. Nohl K, Evans D (2006) Quantifying information leakage in tree-based hash protocols (short paper). In: Ning P, Qing S, Li N (eds) Information and communications security. ICICS 2006. Lecture notes in computer science, vol 4307. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11935308_16
31. Pu C, Li Y (2020) Lightweight authentication protocol for unmanned aerial vehicles using physical Unclonable function and chaotic system. In: 2020 IEEE international symposium on local and metropolitan area networks (LANMAN), pp 1–6
32. Rahman F, Bhuiyan MZA, Ahamed SI (2017) A privacy preserving framework for RFID based healthcare systems. Futur Gener Comput Syst 72:339–352
33. Rais RNB, Akbar MS, Aazam M (2018) Fog-supported internet of things (IoTs) architecture for remote patient monitoring systems using wireless body area sensor Networks. In: 2018 IEEE 16th Intl Conf on dependable, autonomic and secure computing, 16th Intl Conf on pervasive intelligence and computing, 4th Intl Conf on big data intelligence and computing and cyber science and Technology, pp 1–5
34. Ray BR, Abawajy J, Chowdhury M, Alelaiwi A (2018) Universal and secure object ownership transfer protocol for the internet of things. Future Gener Comput Syst 78:838–849
35. Saha HN, Auddy S, Pal S, Kumar S, Pandey S, Singh R, … Saha S (2017) Health monitoring using internet of things (IoT). In: 2017 8th annual industrial automation and electromechanical engineering conference (IEMECON), pp 1–5
36. Sedik A, Hammad M, Abd El-Samie FE et al (2021) Efficient deep learning approach for augmented detection of coronavirus disease. Neural Comput Appl
37. Shanin F, Aiswarya Das HA, Arya Krishnan G, Neha LS, Thaha N, Aneesh RP, Jayakrishan S (2018) Portable and centralised E-health record system for patient monitoring using internet of things(IoT). In: 2018 international CET conference on control, communication, and computing (IC4), pp 1–6
38. Simplicio MA Jr, Silva MVM, Alves RCA, Shibata TKC (2017) Lightweight and escrow-less authenticated key agreement for the internet of things. Comput Commun 98:43–51

39. Simplicio M, Oliveira B, Barreto P, Margi C, Carvalho T, Naslund M Comparison of authenticated-encryption schemes in wireless sensor networks. In: Proceedings of the 36th IEEE conference on local computer networks (LCN), Bonn, Germany, 4–7 October 2011, pp 454–461
40. Stergiou CL, Psannis KE, Gupta BB (2021) IoT-based big data secure management in the fog over a 6G wireless network. IEEE Internet Things J 8(7):5164–5171. https://doi.org/10.1109/JIOT.2020.3033131
41. Tewari A, Gupta BB (2018) Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Futur Gener Comput Syst:1–33
42. Uddin MS, Alam JB, Banu S (2017) Real time victim monitoring system based on internet of Things. In: 2017 4th international conference on advances in electrical engineering (ICAEE), pp 1–6
43. Wan J, Al-awlaqi AAH, Li M et al (2018) Wearable IoT enabled real-time health monitoring system. J Wireless Com Network 2018:298
44. Whitmore A, Agarwal A, Xu LD (2015) The internet of things: a survey of topics and trends. Inf Syst Front 17:261–274
45. Wu F, Xu L, Kumari S, Li X, Das AK, Shen J (2018) A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. J Ambient Intell Humaniz Comput 9(4):919–930
46. Yang Y, Ma M (2016) Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. IEEE Trans Inf Forensics Secur 11:746–759
47. Yang J, Li J, Niu Y (2015) A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Syst 43–44:74–86
48. Yang Y, Zheng X, Tang C (2017) Lightweight distributed secure data management system for health internet of things. J Netw Comput Appl 89:26–37
49. Yao X, Chen Z, Tian Y (2015) A lightweight attribute-based encryption scheme for the internet of things. Future Gener Comput Syst 49:104–112
50. Yew HT, Ng MF, Ping SZ, Chung SK, Chekima A, Dargham JA (2020) IoT based real-time remote patient monitoring System. In: 2020 16th IEEE international colloquium on signal processing & its applications (CSPA), pp 1–4
51. Yu C, Li J, Li X, Ren X, Gupta BB (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer-generated hologram. Multimed Tools Appl 77:4585–4608
52. Zhao S, Aggarwal A, Frost R, Bai X (2012) A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Commun Surv Tutor 14:380–400
53. Zhou Z, Huang D, Wang Z (2015) Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. IEEE Trans Comput 64:126–138

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Mohammed Imtyaz Ahmed has 10 years of experience in IT field as technical test lead in various MNC companies in India and he pursed Master of Technology in Telecommunication and software engineering from BITS Pilani, Rajasthan, India in 2015 as part of work integrated programme and Bachelor of Technology in Electronics and Communication Engineering from Jawaharlal Nehru Technical University, Hyderabad, India in year 2011. He is currently pursuing Ph.D. in B.S. Abdur Rahman Crescent Institute of Science & Technology Chennai, India. His main research work focuses on Internet of Things (IoT), Wireless communication.

G. Kannan received Ph.D. degree from Anna University Chennai, India, an M. Tech Embedded Systems from SASTRA University Thanjavur, and B.E Electronics and Instrumentation Engineering from Bharadhidasan University Tiruchirappalli in 2014, 2005 and 2000 respectively. At present he is working as Associate Professor in the Department of Electronics and Communication Engineering of B.S. Abdur Rahman Crescent Institute of Science and Technology Chennai, India. His areas of research include Wireless Sensor Network, System level power management in Embedded systems and Real Time Operating Systems.