LSITA: An Integrated Framework for Leveraging Security of Internet of Things Application with Remote Patient Monitoring System

Mohammed Imtyaz Ahmed (mdimtyazahmed@gmail.com)
B.S. Abdur Rahman Crescent Institute of Science and Technology
G. Kannan
B.S. Abdur Rahman Crescent Institute of Science and Technology
Subba Rao Polamuri
Kakinada Institute of Engineering and Technology

Research Article

Keywords: Leveraging Security, Integrated IoT Security Framework, Secure IoT End to End Communications, Key Sharing, Remote Patient Monitoring System

Posted Date: August 17th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1948226/v1

Mohammed Imtyaz Ahmed[a], G. Kannan[b], Subba Rao Polamuri[c]

[a]Ph.D Scholar, ECE Dept, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India.
[b]Associate Professor, ECE Dept, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India.
[c]Associate Professor, CSE Dept, Kakinada Institute of Engineering and Technology, East Godavari, Andhra Pradesh, India.

mdimtyazahmed@gmail.com[a], kannann@crescent.education[b], psr.subbu546@gmail.com[c]

LSITA: An Integrated Framework for Leveraging Security of Internet of Things Application with Remote Patient Monitoring System

Abstract

Internet of Things (IoT) applications are growing in popularity and utility leading towards more comforts and conveniences with diversified use cases. However, there are security concerns as IoT technology is made up of heterogeneous devices, protocols and standards. Therefore, the environment might have inherent security issues due to lack of an integrated security framework. Security of internet of things applications is thus crucial for the growth of such applications in the real world. Towards this end, we have proposed a series of security schemes in our prior work. In this paper, we proposed an integrated framework for Leveraging Security of Internet of Things Application (LSITA) with Remote Patient Monitoring System (RPMS) use case. The framework is named as Integrated IoT Security Framework which is realized with different schemes to have privacy and end to end security. The framework enables cloud assisted authentication, secure communications among parties involved in IoT application and an improved key sharing model for multi-user data analytics environment. Different security schemes work together with seamless integration. Remote Patient Monitoring System is the case study built to evaluate the proposed framework. Empirical results revealed that the proposed framework has holistic approach to security of IoT applications. It has potential to trigger further research in the area of IoT security.

Keywords – Leveraging Security, Integrated IoT Security Framework, Secure IoT End to End Communications, Key Sharing, Remote Patient Monitoring System

1. Introduction

Smart portable gadgets allow Machine-to-Machine (M2M) integration without human contact. Internet of things is an outcome and connects computers with real-world items. Physical and digital can coexist. IoT-based infrastructure can build a smart dwelling, city, e-governance system, etc.

Cloud computing enables IoT applications. Without cloud computing, IoT use cases cannot be implemented. IoT sensors and networks generate cloud data. Cloud storage makes storing and processing IoT data easier. This study includes cloud computing. Cloud computing reduces geographical and temporal restrictions with scalability, availability, and elasticity.

In an IoT-integrated smart application, RFID technology tracks thousands of objects [1-4]. RFID tags help secure many smart IoT applications. They are related to data-getting hosts. Only those who require the information should have access to it. Authentication must employ RFID tags. RFID poses security and privacy problems. Replay and DoS attacks are hazards [5-6].

We introduce a new RFID-based cloud-assisted authentication solution to solve security problems. In this system, the RFID tag, reader, backend server, and ACS all function together. Hacked RFID tags jeopardize security and privacy. RFID authentication should allow mutual authentication, tag anonymity, availability, forward security, scalability, and secure localization. It is important to keep RFID position information private and prevent tampering with position-related communications. This study addresses all these issues. Here are our paper contributions:

We built and deployed an IoT scenario using RFID-based cloud-assisted authentication for a smart home.

A. Distributed model proves idea. The proposed technique outperforms the present ones, according to experiments.
B. The security and privacy-protected authentication established can help future smart home applications. The presented approach demonstrates scalability, forward security, mutual authentication, tag anonymity, and availability as use RPM use case.
C. Secure end to end communications and data analytic in IoT application using IBM Watson platform.

Rest of paper: Section 2 reviews IoT security concerns, existing solutions, and cloud-based authentication protocols. Describes the proposed system, including an issue description, system model, and secure communication mechanisms. Section 3 inspiration outline to contribute this study to develop security framework. Section 4 of the article shows a proposed methodology for IoT leverage security framework of IoT applications with RPMS as use case. Section 5 includes experiment results and their evaluation using the latest solutions. Section 6 lists prospective research possibilities and summarizes the findings with conclusion.

The internet has changed global information sharing. The internet of things promotes the seamless integration of digital devices and things. It can encompass everything worldwide. This technology is used for smart cities, residences, transportation, and agriculture [7]. IoT affects many businesses. In healthcare, its sensor network allows for real-time health monitoring. IoT security worries abound. Methodological, organizational, and technical. Methodology encompasses process models, run-time protection, control priorities, and assurance methodologies. Cyber security policies, standards, and goals for third-party components are "Organizational" Technical issues include data flows, distributed systems, physical limits, resource constraints, data security, and IoT design. [8].

IoT security, standards, information-centric networking, and interoperability are insufficient, according [9]. Frameworks [10, 11] and security and privacy issues [12, 13] provide IoT security. [14] shows that conventional RSA is too hefty for IoT devices. DH and ECDH are lightweight and vulnerable to replay and man-in-the-middle (MITM) attacks.

Rapid development of mobile and networking technology has led to many applications and services. These applications employ 4G LTE, Zigbee, Bluetooth, and Wi-Fi. These are popular mobile communication technologies. Remote medical care is an example [15-16]. Governments have created health-care plans for an aging population. Wireless technology, sensors, actuators, and the internet of things can form a whole medical network [17]. Medical and healthcare IoT applications will benefit [18].

The medical business manages and tracks drugs using Information Technology. RFID does this. Uniquely identifies patients, blood samples, and patient information. Effective monitoring of elderly and children is also possible [19-23]. Therefore, improving healthcare quality is urgent. These folks must receive healthcare without hospitalization. Mobile healthcare services, GPS location, rural healthcare, wheelchairs, virtual controlling etc. enable remote medical monitoring.

2. Related work

This section presents IoT, RFID-based authentication, and wireless communication research vs IoT.

Wireless connections are crucial to implementing the internet of things, especially with new technology. [24] researchers studied how 5G wireless communications could be used. They expected 5G networks could handle future traffic surges. They also help integrate access technologies. 5G wireless networks are expected to offer speed and a rich user experience. IoT uses wireless technologies. WiMax, WiFi, 3G, 4G, 5G, ZigBee, and IPv6

[25]. Internet of things incorporates nano communications and wearable sensors with bio-medical healthcare and other businesses [26-27]. IoT-enabled gadgets support M2M. This purpose requires protocols and standards [28]. WiFi, Zig Bee, Z-Ware, Bluetooth, 6LoWPAN, IEEE 802.15.3a, En Ocean, Wave2M, RFID, and ONE-NET [29].

5G can capture spectrum and energy for smart applications. 5G communication technology includes energy-harvesting CR devices, D2D networks, pico cell networks, fem to cell networks, and macro cell networks [30]. Wide-area wireless IoT communication is problematic. Small payloads, many devices, bursty demand, higher range, improved energy efficiency, and decreased cost are concerns [31]. Touch and actuation communications are possible with 5G cellular networks. IoT is wireless. WSNs are commonly used [32]. Wireless communications economic impact on smart applications [33]. IEEE 802.15.4, low-power WiFi, and low-energy Bluetooth link smart devices.

Smart wireless applications face challenges. LOS and connectivity issues [34]. Rapid prototyping wireless networks can assist IoT use cases [35]. IoT applications require energy-efficient wireless connectivity. Because wireless devices may be battery-powered, the network is lifespan is shortened [36-38]. Smart grids for IoT require Wi-Fi, Bluetooth, ZigBee, and 6LoWPAN [39]. Nano wireless communications will be essential for smart applications like robots [40]. Wireless communication security includes authentication, secrecy, integrity, authorization, and freshness [41]. Optical wireless communications use infrared and ultraviolet bands [42]. NDN with caching is allowing IoT [43].

Multiple Original Equipment Manufacturer (OEMs) complicate IoT security. Riahi et al. [44] systematically evaluated IoT security. Each IoT-enabled domain has security issues. Security breaches can be caused by many factors. Insufficient security requirements and technology fusion are examples. [45] merges block chain-based distributed ledger

solutions with IoT. IoT-related technologies include Ethereum, and IOTA is Hyper Ledger Fabric. In user-centric IoT case studies with several linked devices, end-to-end connectivity is crucial [46]. Data integrity, web interface, network, application, and device threats are feasible in M2M [47]. Attacks may target different domains. IoT-integrated health care has several drawbacks, including unreliable technology, security issues with web interfaces, insecure mobile and cloud connectivity, and a lack of privacy. Healthcare application vulnerabilities could disclose sensitive data [48].

[49] Sensor, networking, and application layers must all have IoT security. Safe IoT services are essential. [50–52] document IoT application difficulties. Distributed system development might be complicated by communication protocols, limited nodes, and hardware heterogeneity. Model-driven development can improve IoT security [53]. This method lacks the lightweight techniques needed for energy-constrained IoT devices. There are several basic IoT options. Constrained Application Protocol [54] is a protocol (CoAP). DH and ECDH minimize key exchange. They allow MITM attacks. This research improves ECDH to meet security concerns with lightweight protocols.

This section summarizes remote patient monitoring system major contributions. [55] proposed real-time patient monitoring. Instead of transmitting monitoring data, they processed the heart patient's ECG signal. Using MQTT, they posted data. Reduced jitter delay and noise signals. [56] discussed healthcare monitoring architecture. This WBAN-based system uses IoT to monitor oxygen saturation, heart rate, and plethysmogram. The system is performance was evaluated through case study. It improves data dissemination, energy, and stability. IoT was utilized [57] to build a remote patient monitoring system e-Health record system. Their technology monitors foot pressure, temperature, heart rate, and ECG. RFID identifies and verifies people. They said patients should be monitored and communicated with securely. IoT health monitoring system [58]. They used internet-

connected sensors and a sensor network. Smartphone applications can track patients vitals in real time.

Advocated RFID-based IoT authentication in distributed contexts. Authentication using hash functions. Authentication and clustering are included. This method offers mutual authentication, great anonymity, and attack resistance. RFID-based anonymity-preserving medical authentication was presented in [59]. RFID mutual authentication is hash-based. Smart buildings, massive data, and a wireless 6G mobile network might provide a secure environment, according to [60]. This system incorporates edge computing, cloud computing, fog computing and the IoT. [61] uses blockchain to decentralize identification and authorization. It is then added to FIWARE. [62] investigated IoT cross-layer and security issues. Using holograms, chaos, quaternion, and Fresnel transforms, [63] presented four-image encryption. LSTM (Long Short-Term Memory) and CNN were used to detect COVID-19 [64]. [65] studied IoT safety issues. Combining chaotic systems with physical unclonable functions can create a lightweight authentication scheme [66]. Man in the Middle is a UAV attack. They offered a lightweight signature to counter the attack. Random oracle models [67] provided a three-factor IoT security approach. [68-69] offered a privacy-protecting identity-based IoT authentication mechanism. Nodes cannot be physically cloned. IoT components are physically secure. Nasr Esfahani et al. developed end-to-end privacy solutions for IoT-integrated healthcare systems. The approach resisted modification, replay, and man-in-the-middle assaults. According to the literature, IoT has been used for remote health monitoring. RFID-based authentication systems improve IoT security within biomedical systems. WBAN as part of an IoT integrated healthcare system requires improved security and remote patient monitoring system.

3. Inspiration outline

A literature analysis calls for a secure, lightweight IoT platform with reusable building blocks to speed up research. Over the framework, a prototype application conducts an empirical study. Fig. 6 depicts hospital IoT use scenario with RPMS. This inspired the research. Remote patient monitoring is explained.

Method 1: First, do this.

RFID cloud authentication, Multiple parties communicate via cloud-based RFID remote authentication. ACS and backend server are involved.

There is communication within and between networks. Two machines on the same network must use this protocol:

When both are on the same network, they must interact. This enables reader-server communication.

The RFID tag is unique identifier is sent to the reader, then the reader sends the tag is location and V2 information to a backend server. The server then checks the track sequence number. Emergency keys are used if the track sequence number is invalid. The server provides security credentials to the reader in Fig1.

Two backend servers must register mutually to transfer network credentials. ACS can help two networks communicate. ACS is essential for inter-network connections. A reader must connect to an RFID tag to talk to a server. A later ACS transaction reveals another network is underlying database server. ACS is the sole way to learn about a remote database server. The server sends ACS credentials to the reader, who gives them to the RFID tag. The tag connects to another network and sends data and data set for different scenario for Number of tags/readers used in experimental result in Fig 2.

Our cloud-based remote RFID authentication solution has been simulated. Comparing CAS, DAS, and BA Fig. 3 shows the various tag and reader options. The findings of the experiments are recorded.

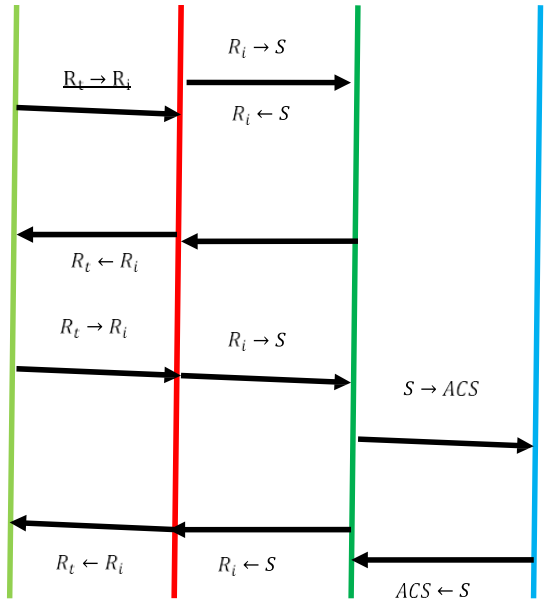

Fig. 1. Cloud-based remote RFID authentication scheme

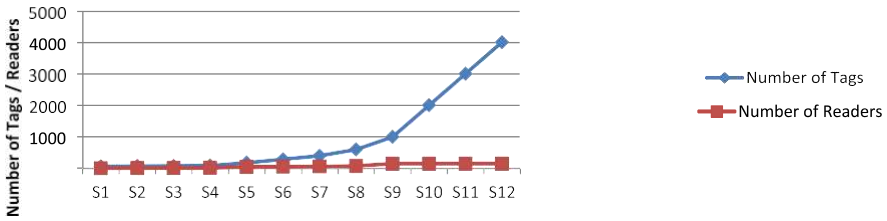

Fig. 2. Dataset used for experiments

Method 2: Enhanced DCDH

ECDH uses lightweight, secure elliptic curves for key exchange. ECDH is lower key length delivers the same security as RSA. ECDH and ECDH-based security methods are lightweight and appropriate for IoT applications with low resources. ECC, part of ECDH, reduces system size. It requires a smaller key size than RSA and offers the same protection. Reduced administrative burden. ECDH works well for IoT applications requiring dynamic key exchange. EC adds algebraically to calculate increments.

E-ECDH has been upgraded from ECDH. It is an elliptic curve optimization.

When comparing security methods like RSA, Diffie-Hellman, and E-E-ECDH (Proposed), the number of bits each key size represents is compared to DES as a baseline. Our calculations show that the suggested system is number of bits per key size beats its competitors. E-ECDH has the highest equivalent bit count with the smallest key size. E-ECDH surpasses RSA, DH, AES, and ECDH.

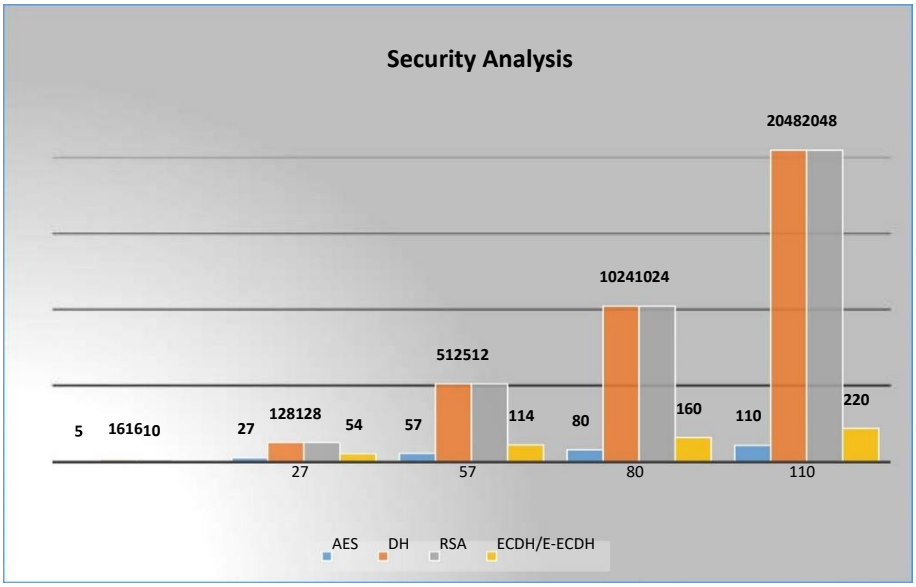

Fig. 3. Performance of security schemes in terms of equivalent number of bits in key size.

Method 3: RPM IOT use case proposed scheme

Section 4 of the RPM use case implementation provides a secure communication approach along with privacy and efficiency with leveraging security of IoT application-RPM.

System design

Based on Section 3 is inspiration outline, this section describes a body sensor, data sender, data receiver, and server. The doctor and patients attendant can see health notifications on their smartphones in Fig. 4.

The Body Sensor monitors a patient's heart rate, blood pressure, and fall risk. A patient's smart watch links it to their body.

Data receivers receive data from body sensors and send it to a server.

The Data Receiver receives data from the Data Transmitter for server analysis. A smartphone application will send patients and carriers test results.

Servers store, analyze, and serve data. Every data transmitter and recipient should register with the server for security and level of privacy in Fig. 5.

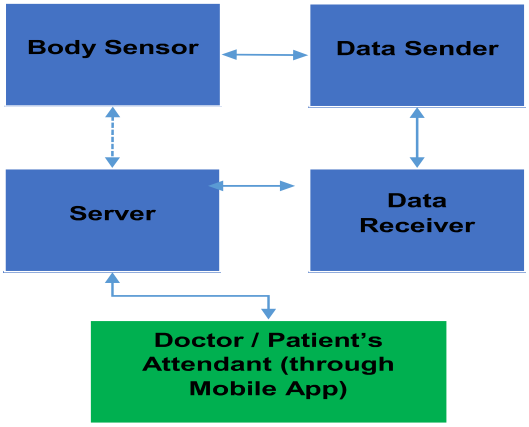

Fig. 4. System architectural overview.

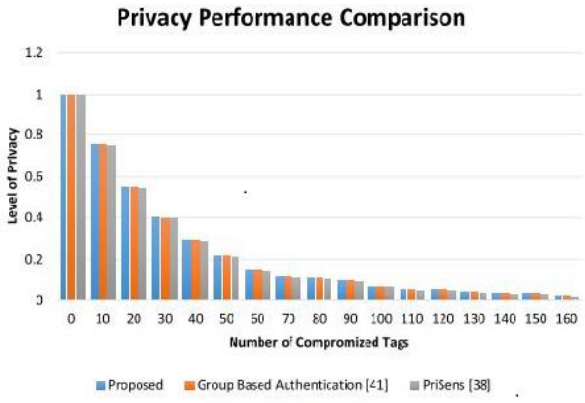

Fig. 5. Level of privacy comparison

Modeling a communication systems design shows how its players interact. The suggested approach protects all participants with lightweight mechanisms. Plan based on Fig. 6 is below.

Two parties can begin their session after authentication. The receiver needs a session key to compute data and update the transaction number indicates limited privacy. Number of compromised tags measures privacy in Fig 5.

Each scheme is number of members. Observe compromised nodes privacy. N individuals equals tags. Changed tags lose systemic influence. Quantify confidentiality levels.

IIoT players must consider security. Energy, Bio-medical healthcare systems, manufacturing, transportation, and government. It is crucial to develop early consensus on IIoT security to avoid security vulnerabilities, especially as systems from different industries interconnect and exploitation efforts are made between them.

This work is based on "Industrial Internet of Things (IIoT) Volume G1: Reference Architecture" (IIRA, [IIC-IIRA2016]), which provides an overview of key architecture components and how they interact. All of them must be protected, together with the system elements that keep them safe.

This document relates to an IIRA security chapter. It delves into security-specific topics to guarantee that security is a design priority.

Annexes cover specialized security topics. One investigates standards and compliance in industrial internet security and covers several recommendations, norms, and laws. Another example explains how to analyze a company is security posture and operations using a maturity model. In the annex, you will discover a list of security

techniques and processes, along with their relevance to important security goals and implementation requirements. This publication is titled "Industrial Internet of Things, Volume G4: Security Framework." This program involves establishing an industry-wide consensus on protecting IIoT systems.

IIoT players must consider security. Energy, healthcare, manufacturing, transportation, and government. It is crucial to develop early consensus on IIoT security to avoid security vulnerabilities, especially as systems from different industries interconnect and exploitation efforts are made between them.

By using SVM kernel classification on gene expression data to examine discrete genetic structures, [70] proposes an enhanced optimal genetic algorithm methodology that might predict malaria infection and uncover new genes.

RPMS reduces hospital expenditures by monitoring patients at home. IoT-based RPMS collects and transmits patient data to remote databases. This data is easily accessible online.

Pharmaceutical Intelligent Information System (PIIS) uses IoT for medicine identification and prescription tracking. This approach can be used to investigate medications for hazardous side effects, renal absorption reactions, pregnancy/breast feeding adverse effects, and specific diseases like tuberculosis.

A home monitoring and decision support system can help clinicians remotely diagnose and treat Parkinson is disease. This method uses an expert system to diagnose and treat patients.

[71] describes health monitoring with the internet of things to investigate smart home data. Remote health monitoring system increases healthcare access and reduces costs.

[72] discusses the creation of an IoT-based mobile gateway for mobile health. The gateway sends caregivers a patient's location, heart rate, and likely diagnosis.

IoT-based health monitoring helps autistic children. A head-worn sensor collects autistic patient's health data. The monitoring server constantly receives these patient's brain data. Inconsistent data triggers a warning and email to the caregiver. In an emergency, doctors are notified. Cloud-based patient data storage offers scalability and effectiveness.

ECGs and other health data can be recorded with mobile devices and sensors and securely uploaded to the cloud, where professionals can access it via an IoT-based healthcare framework (Health IoT) [73]. [74] presents a healthcare solution called Smart Architecture for In-Home Healthcare (SAHHC) that uses photos and facial expressions to monitor patients and the elderly.

[75] proposes an IoT-based ICU monitoring architecture. This paper is methodology can monitor occurrences (abnormalities) quickly and issue timely warnings. IoT-enabled ICUs track significant incidences better than manual and traditional Tele-ICU. Alert creation provides more information and improves the system is benefits.

[76] suggests an IoT-based system for tracking drug use. This paper describes a medicine and a regimen for taking it to increase its effectiveness and lower its cost. In-home monitoring included many monitoring technologies. The monitoring system can use sensors and a wireless module, but they must be safeguarded so health information is not distorted. Internet of things enables device-to-device (D2D) communication, standard messaging, and a communication protocol.

IoT open source cloud efficiently stores sensor data. Digital storage is faster and more reliable than traditional methods in emergencies.

IoT-based patient monitoring is emphasized. IoT-based patient monitoring systems help chronically unwell patients. This strategy entails regularly monitoring patients and providing them control over their food and activity. This study is findings imply that the system is model is equally as effective at changing patient's eating habits as sensors, guidance, and exercise instructions.

[77] IoT-based patient monitoring is proposed. Patient monitoring is linked to IoT. The IoT is more than connected devices. A wireless sensor network can automatically monitor and connect items. Wi-Fi networking makes data collection challenging (sensors). This technique collects and shares patient information with clinicians. Data collection helps increase sensor network energy efficiency and reduce data transmission delays.

[78] suggests a comprehensive patient-monitoring system. Sensors monitor patient's biological behavior. The Internet of things receives biodata. ICU patients can now be monitored in real time, improving efficiency and care. This technology could be turned into a wearable device to monitor old (or) unable-to-care-for children.

[79] uses new technologies and the Internet of things to process a large amount of data. This study focuses on patient's e-health and IoT. Replicating their technique improved patient monitoring and analysis.

[80] shows an IoT-based healthcare monitor. This study proposes an IoT platform for health applications. The device monitors body temperature, heart rate, and blood pressure. Doctors can monitor out-of-clinic test findings in real time.

[81] presents long and short-term memory networks for multi-label classification based on clinical visit records (i.e., time and attention). Both systems help deal with irregular time between therapeutic sessions, but only the second helps determine the relative value of each visit. Based on clinical data from a Southeast Chinese hospital, the proposed technique is superior to traditional and deep learning methods for quick diagnosis.

4. Methodology

The proposed methodology is illustrated.

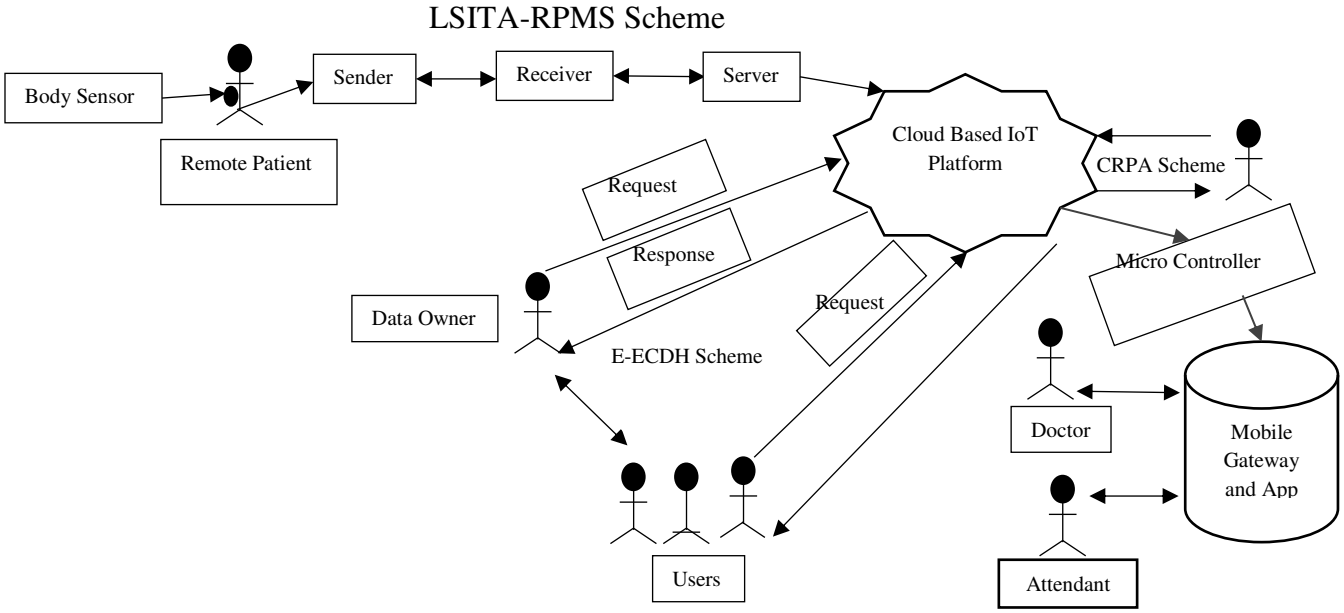

Fig 6. An overview of Integrated Framework for Leveraging Security of Internet of Things Application with Remote Patient Monitoring System (LSITA-RPMS)

This section details the model's design. Diagram of proposed method architecture. Patient data will monitor by doctors and attender while abnormalities in the vital signs and provide the data to authenticate user through cloud server to mobile application with security of Cognitive Robotic Process Automation (CRPA). Patients hospitalized at home (or) in the hospital wear Fig.6. is wrist sensors (Body). Sensors feed cloud servers data. The recommended architecture includes heart rate, body temperature, blood pressure, glucose, stress, and consciousness

sensors. Sensors are wired to a microcontroller. Microcontroller and sensors can communicate over Wi-Fi. Sensors can be utilized without limit.

"Prioritization System" is an IoT-based interface that identifies and sends sensitive data (cloud computing). Next, it labels high-priority material. IoT-based Priority System gathers information, builds a queue based on sensitive and non-sensitive information, and feeds it to the microcontroller at regular intervals. Microcontrollers monitor sensor parameters to communicate patient data to mobile gateway and application (Mobile/Tablet/PDA). Next, send encrypted data to a mobile gateway using Bluetooth (or) Wi-Fi. Mobile gateway has two SIM cards.

Approach outline – LSITA-RPMS:

Following are the method's key components.

Sensors

In [6], three sensors assess patients' health. Instead of [6]'s three sensors, we utilize eight.

Sensor specs:

Heart-rate sensor.

Include temperature sensor.

An EKG.

Glucose sensor.

Stress sensor

Consciousness sensor.

Count pulses.

Accelerometers measure speed.

[6] only uses a pulse counter, accelerometer, and temperature sensor, which can cause treatment issues. This research uses more sensors for a more precise analysis. New architecture has more sensors and a priority system.

Sensors placed on the body to monitor patient's health are crucial, and their priority should be based on their condition. Stress, blood pressure, and body temperature are breast cancer indications. Patients with rare illnesses will also benefit. The priority system allows the mobile gateway and application (e.g. Smartphone/Tablet/PDA) to relay sensor data based on sensitivity. The microcontroller collects heart rate and pulse count data every minute. A sensor measures the patient's temperature every 30 seconds. Other sensors can customize behavior. Data is provided nearby using Bluetooth and Wi-Fi. Enabling this feature reduces data loss and improves data transfer reliability. These sections will elaborate on this issue.

5. Evaluation technique

Logistic regression is regression function is non-linear with the descriptive variables. Pro bit models this interaction in Eq. 1. Classifications use binary variables [82]:

$$bi \in \{-1.\ +1\}. \qquad (1)$$

Bernoulli B random variables may succeed. Key to a project is success is: (a). Using conditional expectation (a), A can be defined as B's predictor in Eq.2 and 3. So, we have

$$E\,[B|A] = \eta(a). \qquad (2)$$

$$g(x) = \ln(3)\, x/\, 1 - x \qquad (3)$$

The logarithmic function is inverse is a logistic function that is chosen as (4): 1

$$h\theta\,(a) = 1 / 1 + \exp\,(-\theta T.\ A) \qquad (4)$$

$$(\theta) = -\left[\sum_{i=1}^{m} \left\{ \begin{matrix} y^{(i)}.\ln\left(h_\theta\left(x^{(i)}\right)\right)+ \\ \left(1-y^{(i)}\right).\ln\left(1-h_\theta\left(x^{(i)}\right)\right) \end{matrix} \right\}\right]. \qquad (5)$$

Loss function is used to optimize model parameters in Eq.5.

When there are multiple data classes, software regression is used. The neural network

architecture used in this study. Feature extraction findings may result in more (or) less than four input layer nerves. Each hidden layer has three layers and three nerves, which may alter based on the network's responsiveness, accuracy, and speed.

Deep learning improves the algorithm. In this way, the LSTM deep neural network algorithm creates a model. The algorithm model is fed data for each test sample.

Neuron scans represent the LSTM algorithm. Each layer is nerve cells are paired using quadratic polynomials. This connection produces new neurons in the next layer. This approach finds a collection of defined functions for an input data vector that can approximate b in Eq 6.

Use A= (a1.a2.a3 an) instead of f to predict b.

M samples from single-output multiple-input data pairs define the following relationships for e: $b_i=f(a_{i1}.a_{i2}.a_{i3}.....a_{in}).\ i=1.2.\ \ M.$ (6)

It is now possible to train an LSTM neural network to predict output values in Eq. 7.

$$A=(a_{i1}.a_{i2}.a_{i3}\ldots a_{in}) \quad (7)$$

Namely: in Eq.8

$$b_i=\hat{f}(a_{i1}.a_{i2}.a_{i3}....a_{in}).i=1.2\ldots.M. \quad (8)$$

For this reason, we must first determine the form of deep neural network to use in order to minimize this square discrepancy between the expected and actual output in Eq.9 :

$$M(\hat{f}ax_i1.a_i2.a_i3.....a_{in}) - b_i)^2 \rightarrow Min. \quad (9)$$

Deep neural networks can represent input-output relationships using complex polynomials. Complex polynomial in Eq. 10, 11 and 12.

$$\hat{y} = a_0 + \sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{m}\sum_{j=1}^{m} a_{ij} x_i x_j + \sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{m} a_{ijk} x_i x_j x_k + \ldots \quad (10)$$

$$\hat{y} = G(x_i x_j) = a_0 + a_1 x_i + a_3 x_i^2 + a_4 x_j^2 + a_5 x_i x_j. \quad (11)$$

$$r^2 = \frac{\sum_{i=1}^{M}(y_i - G_i)}{\sum_{i=1}^{M} y_i^2} \rightarrow Min. \quad (12)$$

Using (13), we get the following matrix equation for each row of M data.

$$Xx = B, \quad (13)$$

In (11), an unknown vector of quadratic polynomial coefficients in Eq. 14

$$x = \{x0.x1.x2.x3.x4.x5\}. \quad (14)$$

$$B = \{b1.\ b2.\ b3.....bM\}^T.$$

Following the least squares approach to multiple regression, solving normal equations can be done in the following manner in Eq. 15.

$$x = (X^{TX}A)^{-1}X^{TB}. \quad (15)$$

Eq. (11) finds the appropriate quadratic coefficients for the complete triple M data set. These equations make this solution error-free. Using this core, models are developed, classified, and patients monitored.

Dataset, This study uses data from patient-connected IoT wrist sensors. IoT devices upload data hourly. Each sample contains more than a terabyte of data each hour. IoT devices deliver data to servers 24/7. Table 1 shows the proposed strategy is dataset.

Table 1 compares 10 people's health in different situations and times of day. During intensive physical exercise (or) sports, tachycardia is not a relevant factor.

Results comparison

This section discusses the model is simulation findings. [83] compares this study is results. This section examines the algorithm is accuracy in different patient states. In our simulation, we compare this criterion to the paper is findings. Accuracy

of the suggested model is demonstrated in the picture, where 8 sensors communicate 100 events per unit of time to the micro controller.

Fig.7 is vertical axis shows patient's health control accuracy, while the horizontal axis shows the medical center's response rate. The proposed model is 100% accurate in 95% of cases. Two-, three-, and four-sensor techniques have 90-10% accuracy. Because the offered method uses IoT and 5G, it is highly accurate. Dual-SIM mobile phones, wireless and wired communication methods also contributed. Fig 8. compares 20 sensors to other techniques.

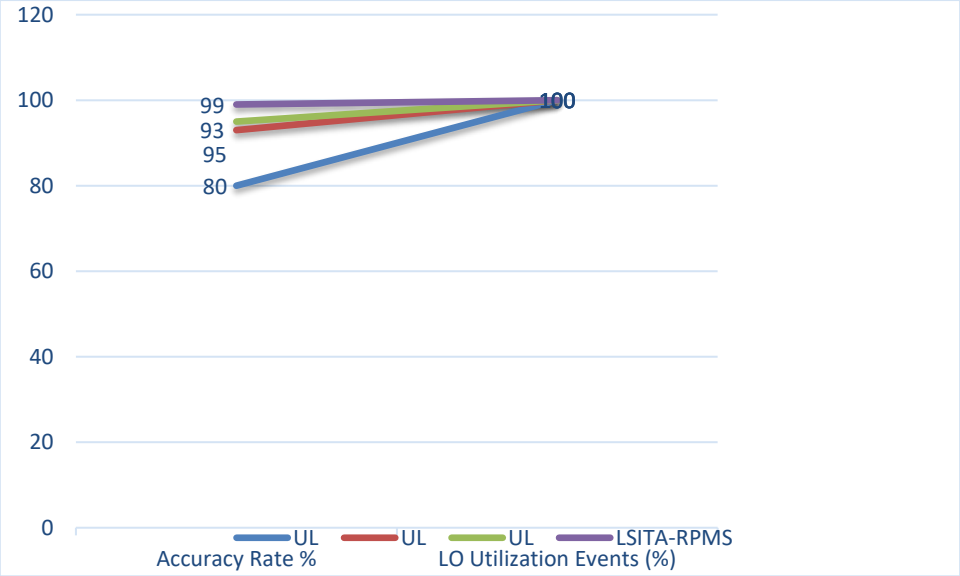

Fig.7. A comparison of the suggested method is accuracy in monitoring patient health with existing approaches utilizing eight sensors

In 95% of situations, sensors communicate and receive data to the medical center accurately and without difficulties.

After removing all the sensors, we could assess the patient's diagnosis. Diagram of proposed method's accuracy diagnosing patient problems.

In 70% and 30% of cases, the proposed technique accurately diagnoses a patient's serious status. To better diagnosis and control of patient's diseases, increase the number of patient sensors.

We compare this study's results with the original's. Here is how the suggested method compares to the reference [72].

Figure 7 demonstrates that the 8-sensor approach has a 97.13% accuracy rate, while [72]'s method has an 89% accuracy rate. These interpretations enhance classification accuracy and patient diagnosis by 10.41% over [72]. Table 1 compares the suggested method's accuracy, precision, and recall to [72] methods.

Table 1 demonstrates that the suggested model is 97.13% accurate at identifying important patients. The proposed method is 10.41% better than SVM, decision tree, KNN, and Nave Bayes [72]. The suggested method detects critical patients with 98.44% accuracy and classifying patient's health status in the proposed model in Fig 9 and the comparison of existing with new proposed scheme improvements in Fig 10.

Comparing the suggested technique based on LTSM deep neural network with According to the following criteria:

Methods	**Accuracy %**	**Precision %**	**Recall %**	**Error %**
SVM	80.0	67	90	30.5
Decision Tree	75.64	68	89	38.08
KNN	83	64	89	32
Naïve Bayes Model	84.90	75.8	86	31.5
Methods [72]	91.5	78	92	23.67
Proposed Method	98.51	99.58	99.61	9.67

Tab 1. The comparison of the proposed method based on LTSM deep neural network with that of [72] in terms of accuracy, precision, and recall.

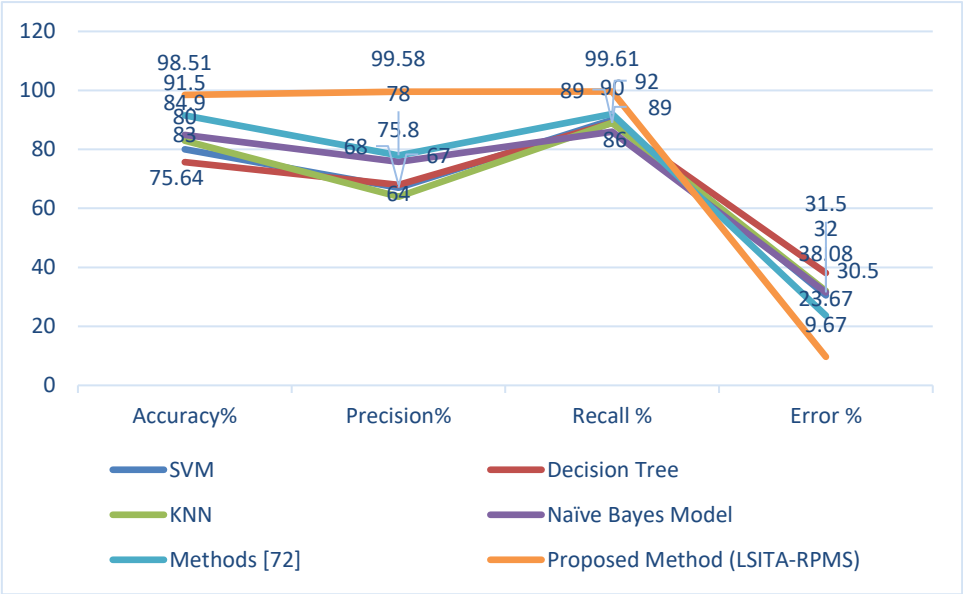

Fig. 8. Results of the accuracy of sending and receiving data from sensors to the hospital in the proposed method using 20 sensors with that of other methods

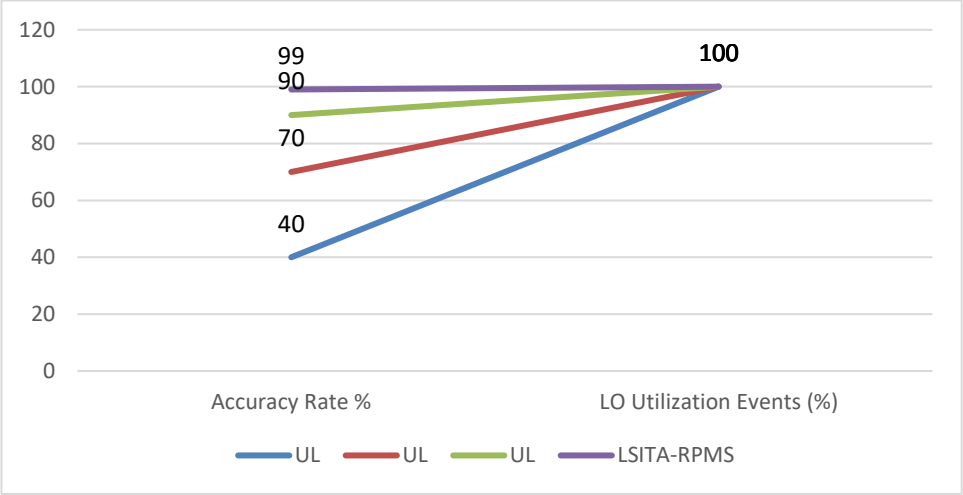

Fig. 9. The accuracy of classifying patient's health status in the proposed model

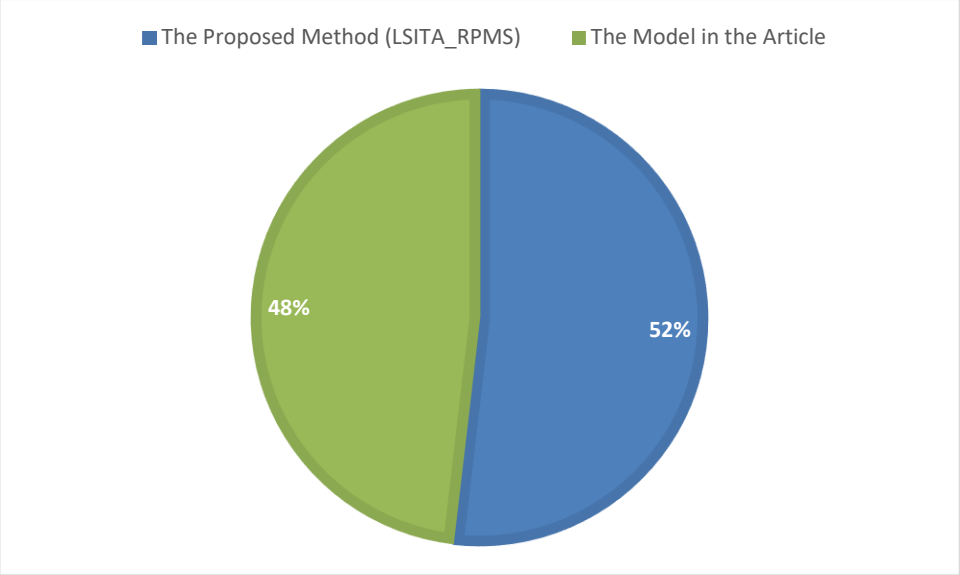

Fig. 10. Comparison of classification accuracy and diagnosis accuracy of the proposed model with those of [72]

SVM, Decision Tree, KNN, and Nave Bayes algorithms have an accuracy rate of 85.59 percent, while the proposed method improves precision by 75.39 percent. The proposed technique identifies 90.93% of people with critical health conditions. The suggested method represents a 48% improvement over SVM, decision tree, KNN, and Nave Bayes.

6. Conclusion and Future work

E-ECDH solves ECDH's security flaw to protect IoT-connected digital infrastructure. The proposed scheme outperforms state-of-the-art approaches, according to empirical research. Future IoT security improvements will address applications from different sectors. RFID-based remote RFID authentication with untraceability, forward secrecy, and anonymity was presented. IBM Watson IoT is connected with a healthcare application for an empirical investigation. This study article also presents a comprehensive proposal (LSITA-RPMS), whose implementation in fog and edge computing with the biomedical

industry is possible in the future. This proposal takes into account all fundamental security needs to be satisfied.

Ethics Declarations:

Ethical Approval and Consent to Participate

Not Applicable.

Human and Animal Ethics

Not Applicable.

Consent for Publication

Not Applicable.

Availability of Supporting Data

Not Applicable.

Competing Interests

The authors declare no potential conflicts of interest with respect to the research, authorship, publication of this article.

Funding

Not Applicable.

Author's Contributions

All authors reviewed the manuscript.

Acknowledgements

Not Applicable.

Author's Information

Mohammed Imtyaz Ahmed

Ph. D Scholar, ECE Dept, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India. ORCID: 0000-0003-4794-7683

G. Kannan

Associate Professor, ECE Dept, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India.

Subba Rao Polamuri

Associate Professor, CSE Dept, Kakinada Institute of Engineering and Technology, East Godavari, Andhra Pradesh, India.

Corresponding Author

Correspondence to **Mohammed Imtyaz Ahmed**

7. References:

1. Muhammad, RA, MBI Reaz and MA Mohd Ali (2012). A review of smart homes – past, present, and future. In *IEEE*, pp.1–12.
2. Kounelis, I, G Baldini, R Neisse, G Steri, M Tallacchini and A^ G Pereira (2014). Building trust in the human– internet of things relationship. In IEEE, pp. 1–9.
3. Gope, P, R Amin, SK Hafizul Islam, N Kumar and VK Bhalla (2017). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Generation Computer Systems, 1–10.
4. Ahmed,IandGKannan(2018).Areviewonpresentstate-of-the-artonInternetofThings.Journal of Advanced Research in Dynamical and Control Systems, 352–358.
5. Feldhofer,M,MAigner,TBaier,MHutter,TPlosandEWenger (2010). Semi-Passive RFID Development Platform for Implementing and Attacking Security Tags, pp.1–6.
6. Zhang, K, J Ni, K Yang, X Liang, J Ren and X (Sherman) Shen (2017). Security and privacy in smart city applications: Challenges and solutions. In IEEE, pp. 1–8.
7. Baranwal, Nitika, T., & Pateriya, P. K. (2016). Development of IoT based smart security and monitoring devices for agriculture. In 2016 6th international conference—cloud system and big data engineering (Confluence) (pp. 1–6).
8. Duc, A., Jabangwe, R., Paul, P., & Abrahams son, P. (2017). Security challenges in IoT development: a software engineering perspective. Proceedings of XP2017 Scientific Workshops, ACM, 1–5.
9. Datta, S. K., & Bonnet, C. (2016). Easing IoT application development through data tweet framework. In 2016 IEEE 3rd world forum on internet of things (WF-IoT) (pp. 1–6).
10. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of things: A survey on the security

of IoT frameworks. Journal of Information Security and Applications, 38, 8–27.

11. Kang, Y.-M., Han, M.-R., Han, K.-S., & Kim, J.-B. (2015). A study on the internet of things (IoT) applications. International Journal of Software Engineering and Its Applications, 9(9), 117–126.
12. Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. D. (2018). Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities. ACM Computing Surveys, 52(4), 1–39.
13. Ahmed, M. I., & Kannan, G. (2020). Overcoming privacy and security challenges of internet of things applications. International Journal of Future Generation Communication and Networking, 13(1), 1550–1556.
14. Jonsson, F., & Tornkvist, M. (2017). RSA authentication in internet of things. http://www.diva-portal. org/smash/get/diva2: 1112039/FULLTEXT01.pdf.
15. Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., 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.
16. Simplicio Jr., M.A., Silva, M.V.M., Alves, R.C.A., Shibata, T.K.C., 2017. Lightweight andescrow-less authenticated key agreement for the Internet of Things. Comput.Commun. 98, 43–51.
17. 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.
18. Ray, B.R., 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.
19. Simplicio, M., Oliveira, B., Barreto, P., Margi, C., Carvalho, T., Naslund, M., October2011. Comparison of authenticated-encryption schemes in wireless sensor networks 4–7, 454–461.
20. Chiuchisan, I., Dimian, M., 2015. 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.

21. Khemissa, H., Tandjaoui, Demissa and Tandjaoui, September 2015. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things 9–11, 90–95.
22. 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.
23. Imtyaz Ahmed, Mohammed, Kannan, G., et al., 2021. Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications. Journal of Information & Knowledge Management (JIKM), 20 (01, 1-20). https://doi.org/10.1142/S0219649221400049.
24. Imtyaz Ahmed, Mohammed, Kannan, G., et al., 2021. Secure End to End Communications and Data Analytics in IoT Integrated Application Using IBM Watson IoT Platform. Wireless Personal Communications. https://doi.org/10.1007/s11277-021-08439-7. In press.
25. Osseiran,A, F Boccardi, VBraun, K Kusume,P Marsch,M Maternia, OQueseth,MSchellmann,HSchotten,HTaoka,HTullberg,MAUusitaloandBog(2014).Scenariosfor 5G mobile and wireless communications, the vision of the metis project. In IEEE, pp.26–35.
26. Xu,LD(2013).Internet of things in industries, a survey. IEEE Transactions on Industrial Informatics, 1–11.
27. Dressler,FandSFischer(2014). Connecting In-Body Nano Communication with Body Area Networks: Challenges and Opportunities of the Internet of Nano Things, pp.1–10.
28. Kannan, G and RM Thameez (2015). Design and implementation of smart sensor interface for herbal monitoring in IoT environment. International Journal of Engineering Research, 469–475.
29. Aijaz, A, M Dohler, AH Aghvami, V Friderikos and M Frodigh (2015). Realizing the tactile internet: haptic communications over next generation 5G cellular networks. IEEE Wireless Communications,1–8.
30. Kuzlu, M, M Pipattanasomporn and S Rahman (2015). Review of communication technologies for smart homes/building applications. In IEEE, pp. 1–6.

31. Liu, Y, Y Zhang, R Yu and S Xie (2015). Integrated energy and spectrum harvesting for 5G wireless communications. In IEEE, pp. 75–81.
32. Dhillon, HS, H Huang and H Viswanathan (2015). Wide Area Wireless Communication Challenges for the Internet of Things, pp. 1–12.
33. Khalil, N, MR Abid and D Benhaddou (2016). Wireless Sensor Network for Internet of Things, pp.1–6.
34. Luong, NC and DT Hoang (2016). Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey, pp.1–45.
35. Ai, B, X Cheng, T Kürner, Z-D Zhong, K Guan, R-S He, L Xiong, DW Matolak, DG Michelson and C Briso-Rodriguez (2014). Challenges toward wireless communications for high-speed railway. IEEE Transactions on Intelligent Transportation Systems, 15(5),2143–2158.
36. Kruger, CP, AM Abu-Mahfouz and GP Hancke (2015). Rapid prototyping of a wireless sensor network gateway for the internet of things using o®-the-shelf components. In IEEE, pp. 1926–1931.
37. Kamalinejad, P, C Mahapatra, Z Sheng, S Mirabbasi, VCM Leung and YL Guan (2015). Wireless energy harvesting for internet of things. In IEEE, pp. 1–19.
38. Liu, Y, A Liu, Y Hu, Z Li, Y-J Choi, H Sekiya and J Li (2016). FFSC, an energy effeciency communications approach for delay minimizing in internet of things. In IEEE 4, pp. 3775– 3793.
39. Mahmoud, MS and AAH Mohamad (2016). A study of e±cient power consumption wireless communication techniques/modules for internet of things (IoT) applications. Advances in Internet of Things, 19–29.
40. Mahmood, A, N Javaid and S Razzaq (2015). A Review of Wireless Communications for Smart Grid. Elsevier, pp.248–260.
41. Boillot, N, D Dhoutaut and J Bourgeois (2014). Using Nano-wireless Communications in Micro-Robots Applications, pp.1–10.
42. Nguyen, KT, M Laurent and N Oualha (2015). Survey on Secure Communication Protocols for the Internet Of Things. Elsevier, pp.17–31.

43. Uysal, M and H Nouri (2014). Optical wireless communications – An emerging technology, 1. In IEEE, pp. 1–7.
44. Hail,MA,MAmadeo,AMolinaroandSFischer(2015).Cachinginnameddatanetworkingforthewirelessinternetofthings.In IEEE,pp.1–6.
45. Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013) A systemic approach for IoT security. DCOSS, Boston, United States (pp. 351–355).
46. Pustišek, M., & Kos, A. (2018). Approaches to front-end IoT application development for the Ethere- umblockchain. Procedia Computer Science, 129, 410–419.
47. Datta, S. K., Gyrard, A., Bonnet, C., & Boudaoud, K. (2015). oneM2M architecture based user centric iot application development. In 2015 3rd international conference on future internet of things and cloud (pp. 1–8).
48. Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 95(1), 169–185.
49. Ahamed, J., & Rajan, A. V. (2016). Internet of things (IoT): Application systems and security vulnerabilities. In 2016 5th International conference on electronic devices, systems and applications (ICEDSA) (pp. 1–5).
50. Liu, Z., & Yan, T. (2013). Study on multi-view video based on IOT and its application in intelligent security system. In Proceedings 2013 international conference on mechatronic sciences, electric engineering and computer (MEC) (pp 1–4).
51. Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Tarquino Murgueitio, D., Garcia, E., Nespoli, P., & Gómez Mármol, F. (2018). Developing secure IoT services: A security-oriented review of IoT plat- forms. Symmetry, 10(12), 1–34.
52. Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
53. AL-mawee, W. (2012). Privacy and security issues in IoT healthcare applications for the disabled users a survey, 1–57.
54. Nguyen, X. T., Tran, H. T., Baraki, H., & Geihs, K. (2015). FRASAD: A framework for model-driven IoT Application Development. In 2015 IEEE 2nd world forum on internet of things (WF-IoT) (pp. 1–6).

55. Ukil, A., Bandyopadhyay, S., Bhattacharyya, A., Pal, A., & Bose, T. (2014). Lightweight security scheme for IoT applications using CoAP. International Journal of Pervasive Computing and Communications, 10(4), 372–392.
56. Yew, H.T., Ng, M.F., Ping, S.Z., Chung, S.K., Chekima, A., Dargham, J.A., 2020. IoT Based Real-Time Remote Patient Monitoring System. 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA). P1-4.
57. Akkas,, M. A., Sokullu, R., ErtürkÇetin, H., 2020. Healthcare and Patient Monitoring Using IoT. Internet of Things, 11, 1–12.
58. Shanin, F., Aiswarya Das, H.A., Arya Krishnan, G., Neha, L.S., Thaha, N., Aneesh, R.P., 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.
59. Saha, H. N., Auddy, S., Pal, S., Kumar, S., Pandey, S., Singh, R., Saha, S. (2017). Health monitoring using Internet of Things (IoT). 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON). P1-5.
60. Wu, F., Xu, L., Kumari, S., Li, X., Das, A.K., Shen, J., 2018. A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. J. Ambient Intell. Human. Comput. 9 (4), 919–930.
61. Christos L. Stergiou, Kostas E. Psannis and Brij B. Gupta. (2020) IoT-based Big Data secure management in the Fog over a 6G Wireless Network, p1-8.
62. Esposito, C., Ficco, M., Gupta, B.B., 2021. Blockchain-based authentication and authorization for smart city applications. Inform. Process. Manag. 58(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468.
63. Tewari, A., Gupta, B.B., 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Gener. Comput. Syst. 108, 909–920.
64. Yu, C., Li, J., Li, X., Ren, X., Gupta, B.B., 2018. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimed. Tools Appl 77 (4), 4585–4608.
65. Sedik, A., Hammad, M., Abd El-Samie, F.E. et al. (2021). Efficient deep learning approach for augmented detection of Coronavirus disease. Neural Comput. Applic.

66. Adat, V., Gupta, B.B., 2018. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun. Syst. 67 (3), 423–441.
67. Pu, C., Li, Y., 2020. Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System. IEEE International Symposium on Local and Metropolitan Area Networks(LANMAN). 2020, P1–6.
68. Rangwani, D., Sadhukhan, D., Ray, S., Khan, M.K., Dasgupta, M., 2021. A robust provable-secure privacy-preserving authentication protocol for Industrial Internet of Things. Peer-to-Peer Netw. Appl. 14 (3), 1548–1571. https://doi.org/10.1007/s12083-020-01063-5
69. Alzahrani, B.A., Mahmood, K., 2021. Provable Privacy Preserving Authentication Solution for Internet of Things Environment. IEEE Access 9,82857–82865. https://doi.org/10.1109/Access.628763910.1109/ACCESS.2021.3086735.
70. Adebiyi MO, Arowolo MO, Olugbara O. A genetic algorithm for prediction of RNA-seq malaria vector gene expression data classification using SVM kernels. Bull Elect Eng Informat. 2021;10(2):1071–9.
71. Puustjärvi J, Puustjärvi L. The role of smart data in smart home: health monitoring case. Proc Comput Sci. 2015; 69:143–51.
72. Santos J, et al. An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. J Netw Comput Appl. 2016;71: 194–204.
73. Shamim Hossain M, Ghulam M. Cloud-assisted industrial internet of things (iiot)-enabled framework for health monitoring. Comput Netw. 2016; 101:192–202.
74. Mano LY, et al. Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. Comput Commun. 2016; 89:178–90.
75. Bhatia M, Sood SK. Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. J Med Syst. 2016;40(8):1–15.
76. Zanjal SV, Talmale GR. Medicine reminder and monitoring system for secure health using IOT. Proc Comput Sci. 2016; 78:471–6.
77. Shaikh S et al. Patient monitoring system using iot. In: 2017 International Conference on Big Data, IoT and Data Science (BID). IEEE, 2017.
78. Uddin MS, Jannat BA, Suraiya B. Real time patient monitoring system based on Internet

of Things. In: 2017 4th International Conference on Advances in Electrical Engineering (ICAEE). IEEE, 2017.

79. Dey N, Ashour AS, Bhatt C. Internet of things driven connected healthcare. In: Internet of things and big data technologies for next generation healthcare. Springer, Cham, 2017. pp 3–12.
80. Tan ET, Abdul HZ. Health care monitoring system and analytics based on internet of things framework. IETE J Res. 2019;65.5:653–60.
81. Rahmani AM, et al. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach. Fut Generat Comput Syst. 2018; 78:641–58.
82. Mutlag A, et al. Enabling technologies for fog computing in healthcare IoT systems. Fut Generat Comput Syst. 2019; 90:62–78.
83. Hinton GE, Salakhutdinov RR. Reducing the dimensionality of data with neural networks. Science. 2006;313(5786):504–7.