Extensive Analysis Of Internet Of Things Based Health Care Surveillance System Using Rfid Assisted Lightweight Cryptographic Methodology

G.S.Gunanidhi[a], R.Krishnaveni [b]
[a] Research Scholar, Department of Computer Science, Hindustan Institute of Technology and Science
[b]Professor, Department of Computer Science, Hindustan Institute of Technology and Science
Email: [a]author1@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Internet of Things (IoT) plays a vital role in Smart Applications such as Smart City Maintenance and Control, Health Care, Transportation, Defense Operations and so on. Compare to all of these mentioned applications Health care is the most significant and necessary application to take care with as well as the concern regarding patients and their belongings need to be monitor the patient health related summary from the remote end without any hurdle. This is possible with the help of Internet of Things, in which it enables the bridge between client end and the server end to track the health records clearly without any delay as well as providing the proper security mechanisms to the health records preserved into the server. In this paper, a new Radio Frequency Identification (RFID) enabled Lightweight Cryptographic Method (RFIDLCM) is introduced to provide proper security mechanisms to the health records preserved into the server end. In addition, it must be kept secure against abuse as well as authentication when storing the patient's record as other devices can easily be monitored. It is quite difficult to encrypt voluminous data encryption protocols because of restricted IoT devices. For this reason, Homomorphic encryption models are recommended and in this paper, a new block cipher technique has been proposed for the safe transmission of health information from such Internet of Things devices. The proposed approach is activated with the help of Smart Helath Monitoring Device interconnected with several health related sensors such as RFID Reader, ECG Sensor, Pressure Level Estimation Sensor and Temperature Sensor. All these sensors are integrated together to provide a proper solution to the health care surveillance scheme in an intelligent manner. The resulting emulations of this paper proves the efficiency of the proposed approach in clear manner with graphical representations. The proposed approach of RFIDLCM proves its efficiency with respect to the improvements in prediction accuracy levels, security levels, time concerns and the data transportation efficiency.

Keywords: Internet of Things, IoT, RFID enabled Lightweight Cryptographic Method, RFIDLCM, Cipher Methodology, ECG

1. Introduction

The main purpose of this device is to track patient health information every instant and monitor the server details by an innovative Internet of Things and care takers can access or follow patients' current position instantly without any secret activities. The ultimate goal is to achieve high precision and speed. Internet of Things is a communications boon that links remote people through the global media. IOT is primarily concerned with allowing a strong network link on small devices with adequate privacy issues. In this system, the focus is focused in the Lightweight RFID Protocol Drug System-based health monitoring with suitable privacy institutions. This method allows the patient's information to be accessed on the global server from a control point of view. With the system no one can trick caregivers, nobody can conceal the patient's medical summary and nobody can know about the patient's real condition. In this scheme, a new cipher framework is implemented with respect to IoT technology for smart and reliable screening with the Lightweight RFID methodology.

Specifically, Flexible RFID Configuration and its implementation technology enables sophisticated health related data propagation strategy in the IoT environment are described in the IoT and health care framework. Large data maintenance strategies are implemented to address the highly complex quantity of predictive analysis mounted in systems, because the huge volume of information captured by sensor system is expansive and rapid than ever. One of IoT's biggest applications today is the health care system and t he IoT enabled health care systems can be seen across the Internet as the field of biomedicine. In health care IoT devices critical data relating to remote health care control, treatment etc. are collected and transmitted to the remote IoT server. It is used for the treatment of patients and eliminates human efforts in electronic health care.

A safe IoT enabled health care system provides greater scope for designing smart health care systems and it would increase healthcare quality with lower costs. This kind of smart Healthcare primarily deals with data relating to storage patients that are highly vulnerable to health care professionals. Users may manage these health related information from anywhere in the world at any time. Because of this strategy, the protection of these confidential medical information are among the most demanding concerns. Appropriate cryptographic techniques are vital for the e-health operational framework on IoT because the resources of these IoT devices are limited. Data protection is essential before data is transferred to the corporate network. Since the memory and processing capacity of the computer is restricted, a suitable lightweight encryption is essential for the data encryption [2][3]. In literature several lightweight block cipher algorithms have been found and i t is very important to create an

energy-efficient block chip technology, as battery capacity is lower in the IoT devices. Several other models are based on the well known block chipers mentioned above can be found in [4]. The paper offers a cryptography technology known as RFID enabled Lightweight Cryptographic Method (RFIDLCM), which is necessary for IoT devices, which is enabled by powerful lightweight IoT. This technique involves low calculation and reduced energy consumption. The results of the implementation show that it is machine efficient

2.Internet of Things

Internet of Things (IoT) is a comprehensive framework that includes many essential technologies and one of the key technologies in IoT architecture is Radio Frequency Identification (RFID). The Classic RFID device consists of the RFID card, reader and server. In this method, tag collects and simple processing information uses the server to process and store the data, and the reader may identify the tag and function as an intermediary to communicate amongst RFID Card and server. RFID is an ID free technology that provides an automatic identification feature, high storage space, portability and safety [1][4] that allows for a friendly application in the medical field. In the health care system, RFID Cards can be attached or inserted on the layer of an entity and collected the related details based on the authentication principles specified. The following figure, Fig-1 illustrates the detailed view of Internet of Things architecture with clear sensor unit specifications.

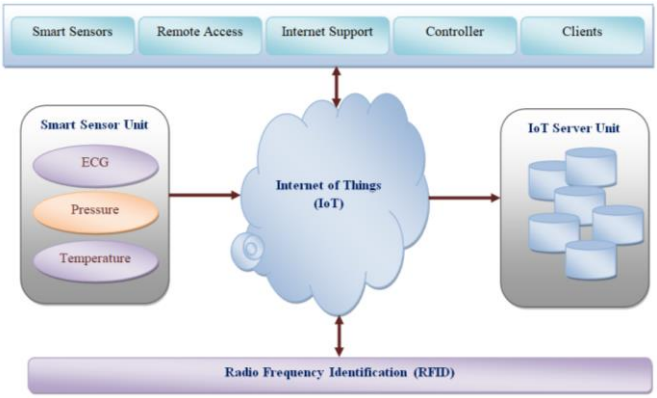


Fig.1 IoT Architectural Perception

The RFID Card will collect physical health information and connect as well as communicate with either the server for patients. It provides remote meaningful communication and health care summary up to a possibility as well as it offers a new technological support for WLAN and smart healthcare applications. Because of these features, the patient approved physician or relatives and friends are able to track the physical health data of the user through the RFID device. Protection problems are part of the advantages of the medical RFID system [2]. Personal physically sound information is understood to be closely linked to personal privacy. The attackers are now infiltrating the cyber world and stealing or falsifying patient privacy data and undermining the normal workflow of the system which results in the serious exposure of client confidentiality data. Security has thus be among the main issues for medical RFID to be handled safely. A novel and flexible RFID authentication system is presented and it is used in a medical context to solve the past communication issues. The proposed schema uses less computational resources and fulfils anonymity, resistance to attacks replay, synchronization, forward protection and mutual authentication, and non-denial of service, based on Tian's protocol.

3.Radio Frequency Identification enabled Health Care Surveillance

Radio Frequency Identification (RFID) methodology is a system that transmits a target to be identified and data to be read automatically and remotely via a radio signal [2]. In particular, RFID has also been generally included in a range of contactless applications, including personal-ID, libraries and access control systems [5]. Importance has been given to RFID for nearly a decade now, which is anticipated to monitor effectively hospitals, medical equipment, medicines and patients [6][7]. Figure 3 presents an RFID assisted medical health care system with RFID tags attached to items such as drug control systems, medical aid equipments, medical devices and even patients.

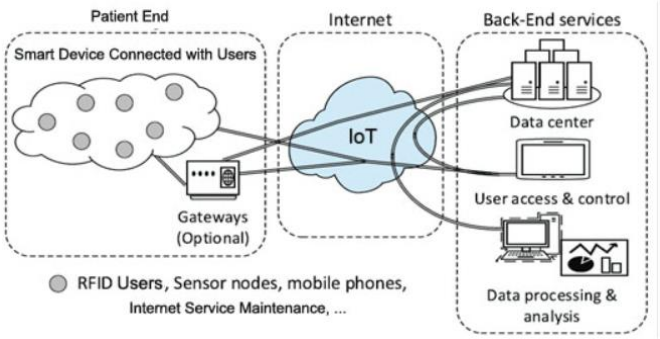


Fig.2 RFIDLCM Architectural Design

In order to really get the valuable knowledge with these items, permanent or lightweight readers may identify these tags and then interact efficiently with the server on some computer terminals. Furthermore, the rightful persons responsible for the various components can access the server information through internet, the entire information being productive and intelligent. For example, a licensed doctor may obtain the vital signs of a patient remotely can offering the helpful information in order for the person to improve quickly. In addition, the patient's family members can also automatically gain health status and connect with either the physicians in period and together they can provide better treatment solutions. The RFID assisted health care scheme therefore provides an excellent method of medical healthcare management and management. In addition, RFID encourages improved control of vital healthcare properties, for example, wheelchairs and medical equipment by allowing real-time detection, monitoring and tracing, in order to prevent any inappropriate medical incidents. Moreover, the successful implementation of Artificial intelligence in the health care sector can provide enormous advantages for performance, quality and management [8].

The remaining portions of this paper describe regarding Related Study over section 2, further section of Section 3 illustrates the proposed system methodologies in detail with proper algorithm flow and the Section 4 illustrates the Result and Discussion portion of the paper and the final section, Section 5 illustrates the concept of Conclusion and Future Scope of the proposed paper. These all will be explained in detail over the further section summaries.

4.Related Study

Indrajit-Banerjee et al., 2020 [4] proposed a paper related to IoT assisted Wireless Sensor Networks based smart health care services based on Free-Routing-Techniques. In this paper [4], the authors described such as the Internet of Things topology is recently been used to capture physical, physiological and vital signs from patients in consumer-centered e-health and/or wellness services. Various medical sensors are connected in such health care services to the patients to capture health status from those under surveillance. The data collection phase in the IoT assisted WSN. assisted The effect is a reduction in reliability and regression in IoT assisted Wireless Sensor Network on missing packets and this article [4] introduces a distributed communication protocol for IoT assisted Wireless Sensor Networks in order to overcome congestion for medical applications effectively. The proposed scheme reduces congestion through a priority data routing strategy. In addition, this article includes a priority queue-based scheduling for increased reliability. We mathematically analyze the properties and the feasibility of the algorithm congestion control mechanism through comprehensive simulation and real-life observations. An alarm signal is being used to monitor irregular heartbeat, body temperature, ECG and so on for state-of-the-art diagnosis in the healthcare setting.

Anish Jindal et al., 2020 [5] proposed a paper related to a differentiated Blockchain strategy to edge imagined process over IoT health care services. In this paper [5], the authors described such as the home based health surveillance sensors form a broad Artificial intelligence and IoT network, in which it monitors and sends information continuously to neighboring nodes or servers. The synchronization of these IoT assisted sensors with various entities furthermore leads to security breakdowns whereby the opponent may circumvent the limitations related to data exposure. This is particularly relevant in the healthcare field, where changes in sensor data values can alter the direction of diagnosis, which can cause serious medical problems and therefore introduce a differentiated Permission Blockchain in the edge imagined environment to avoid data tempering and protect patient privacy. This approach leverages surrounding virtualized resources to construct Blockchain blocks, so that the health data can be securely transmitted from sensors to edge nodes. The edge-processors then distribute and preserve cloud data using the tensor-based exponential method. This leads to reducing the replication of data transmission in the massive IoT medical network. The findings indicate the efficacy of the procedure developed with respect of the block preparation, header source level, vectorized-error correction and interpretation flaw.

Chunkai-Qiu et al., 2020 [6] proposed a paper related to Rigid Flex Health care Surveillance and Sensor Update for IoT enabled systems. In this paper [6], the authors described such as the IoT is a revolutionary technology in communication that can link elements from different fields through the Internet. In a new healthcare industry one of the most enticing IoT applications is the conventional medical system, which increasingly demands social services, including physicians, nurses, hospital beds and health monitoring equipment. In this article [6], the concept of a lightweight wearable sensor patch is presented for observations of different physiological parameters, like the electrocardiogram, PPG and body temperature. With ECG and PPG sensors built into the same system, the proposed sensor patches can be used to continuously approximate blood pressure based on pulse time of arrival (PAT) without additional wires and devices. The sensor pad contains a center panel for signal collection and processing, a control platform for power supply and battery charging, and three modules for the monitoring of vital signs. All components have a rigid-flex structure that can be connected securely to the human body for personalized healthcare applications. For custom calculations with a certain feature extraction technique, the sensors can be unlocked from the centre board to minimize power consumption. The efficiency of the suggested sensor patch is validated by experiments compared to the commercial reference unit. The proposed sensor device will communicate physiological parameters electronically to the gateway using a highly advanced Bluetooth low-energy module. From both the sensors patch and gateways encryption keys is implemented to secure the information for privacy and protection during transmission. Both a Smartphone based mobile gateway and stationary endpoint form a connection between all the connected sensing element and the Cloud to store and further analyze health information.

Neeraj-Kumar et al., 2020 [7] proposed a paper related to Blockchain enabled secure authentication in IoT oriented electronic Health care applications. In this paper [7], the authors described such as Bitcoin revolution's recent progress has propelled limitless possibilities for future digital ecosystem design. Bitcoin-owned transactions are completely supported, implemented as well as propagated by a range of revolutionary different temperatures on network technologies in the Blockchain context. While using smart applications in the full niche of the Internet of Things (IoT), such Bitcoin transactions raised the problem of resource-constrained tool sets that were not supported and called for a new architecture. In direct proportion to changes, this article proposes a new Blockchain lightweight IoT Component optimization method while incorporating an improved e-health application simplified payment verification process. This paper first formulates required context arts models, which include the in homogenic Poisson point method, assumption states structure formulation, the relationship between height and depth, the flower filter mechanism, the base stack pay to public key hash and transaction management. Secondly, many main protocols and related processes are used to implement built models. Finally, the review and discussion includes block confirmation time, adequacy of Byzantine tolerance of faults, intelligent contract policy, and the response of the SPV in the proposed scenario.

5.Proposed System Methodologies

Nowadays there seems to be no automatic health care system dependent on drug monitoring. All are performed manually and the system is supervised using man power alone. Massive machineries are used in hospitals to track patient records, which require enormous amount of space and power during processing. Compared to the new technology like the Internet of Things, productivity is so low. There are many drawbacks in the past method of health application, which are described below:

(a) There is just no proper method of intimation and the patient must be tracked and the data recorded by big devices.

(b) There are limited hospital services, access and variety available so caregivers can only ask doctors about patient specifics and would have to believe them.

(c) Massive cost and longer spending.

(d) Data security does not prominence like RFID and everything.

A new RFID based preventive measures on health care are characterized through the use of modern technology, known as RFID enabled Lightweight Cryptographic Method (RFIDLCM). This is an effective monitoring system that tracks patients' on-time medical information without the intervention of an infant or any other attendant who tracks them, instead of using the conventional GPRS system, an effective IoT Module is utilized to provide internet services and to preserve privacy using lightweight techniques based on this approach. With this consumer the health data of patients can easily be monitored from anywhere, using IoT technology. In-house human behavior identification and classification requires this method, even patients can be tracked without any limitations in any situation. This system can be used so conveniently and its function is too user friendly with its accessibility and expense. This technology uses Global Connectivity with small devices that use less electricity. There are many benefits to this proposed solution that are described below:

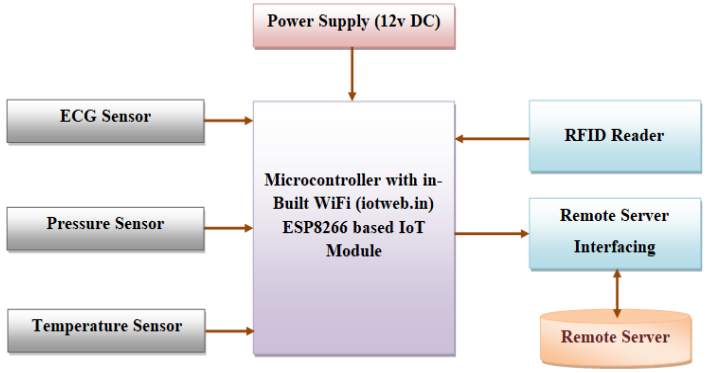
(a) Simplicity, low price versatility and this system can be used by ordinary people, particularly children and the elderly, and does not require special training.

(b) Low electricity consumption.

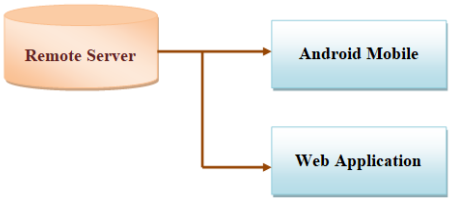
(c) Size compatible.

(d) Security shall be defined via the Lightweight RFID Protocol to ensure proper protection of privacy.

The following figure, Fig-3 (a) illustrates the master block diagram of the proposed approach and the figure, Fig-3 (b) illustrates the slave block diagram of the proposed approach.



(a)



(b)

Fig.3 RFIDLCM Block Diagram

(a) ECG Sensor: The ECG Sensor is used to measure the functioning of heart and generally an electrocardiogram (ECG) is a check that tests the functioning of person's heart by evaluating the heart's electrical activity. An electrical signal passes through your heart with every heart beat. This ripple allows the muscles to compress and circulate the heart's blood. This ECG sensor estimate the value of heart rate and the blood flow conditions in clear manner.

(b) Pressure Sensor: The Pressure Sensor is used to measure the Blood Pressure (BP) rate of the patient, in which a pressure sensor is a gaseous or liquid pressure measuring unit. Pressure represents the force necessary to prevent expansion of a fluid and is generally indicated in pressure is defined. A pressure sensor normally serves as an amplifier; it produces a signal based on the applied pressure. This Pressure sensor estimates the value of both low and high pressures in clear manner and provides the results to the controller in analogue format.

(c) Temperature Sensor: The temperature sensor is used to measure the body temperature and it is an electronic system that monitors temperature of the connected human body and translates input data into electronic data for tracking, monitoring and signaling changes. Many types of temperature sensors are available. In this application DS18B20 temperature measurement sensor is utilized to measure the temperature readings of the patient.

6.Results and Discussions

In this paper a new health care monitoring system is introduced with powerful RFID strategies, which is called as RFID enabled Lightweight Cryptographic Method (RFIDLCM). This system adopts several latest technologies to provide a sufficient support to monitoring the respective patient's health care details in clear manner with proper specifications. This system is composed based on several intelligent sensors and these are all accumulated into the Smart Health Monitoring Device, in which it requires 12V DC power supply to operate as well as the size of the device is too compact. The cipher maintenance schemes are proper in this approach because it utilizes the

Lightweight Cryptographic Methodology to encrypt the health records and maintain that into the server for monitoring. The RFID scheme is used to identify the respective users and provides the proper credentials to access the system accordingly. The following figure, Fig-4 illustrates the security level performance of the proposed approach, in which it shows the cipher accuracy measurements of the proposed approach. This proposed approach of RFIDLCM is cross-validated with the classical RSA encryption algorithm and the proposed approach proves the efficiency level in clear manner.

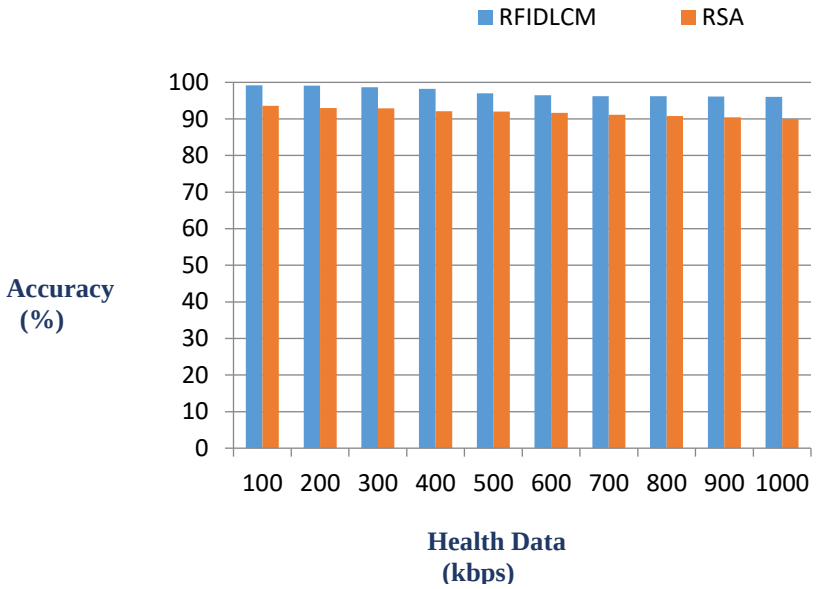


Fig.4 Cipher Efficiency of the Proposed Approach

The following figure, Fig-5 illustrates the prediction accuracy levels of the proposed approach, in which it shows the accurate measurements of the disease based on the patient report as well as the proposed approach of RFIDLCM is cross-validated with the classical SVM algorithm and the proposed approach proves the efficiency level in clear manner.

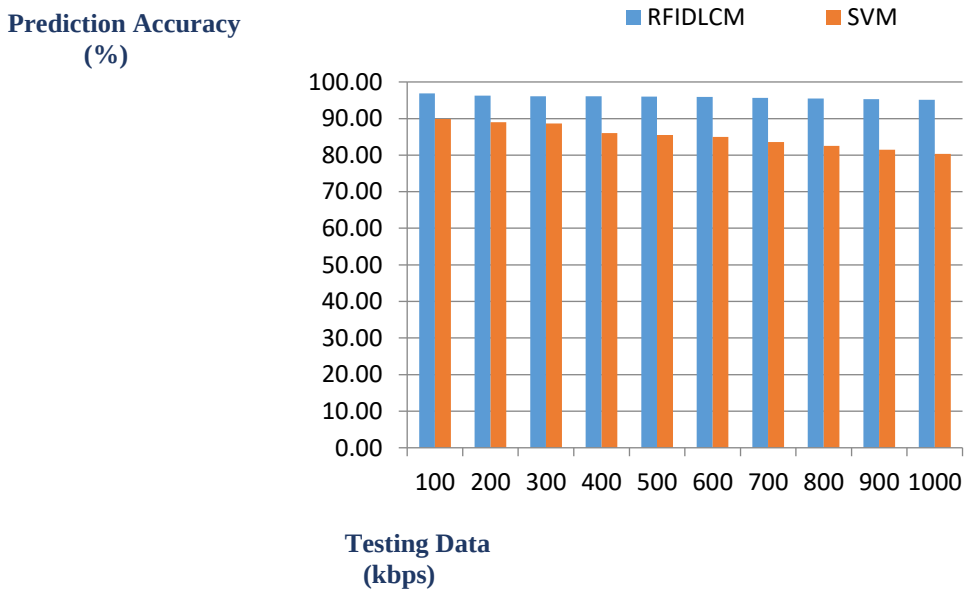


Fig.5 Prediction Accuracy

The following figure, Fig-6 illustrates the processing time efficiency levels of the proposed approach, in which it shows the accurate measurements of the time required to process the total records maintained into the remote server with respect to the testing data given from the patient end as well as the proposed approach of RFIDLCM is

cross-validated with the classical SVM algorithm and the proposed approach proves the efficiency level in clear manner.

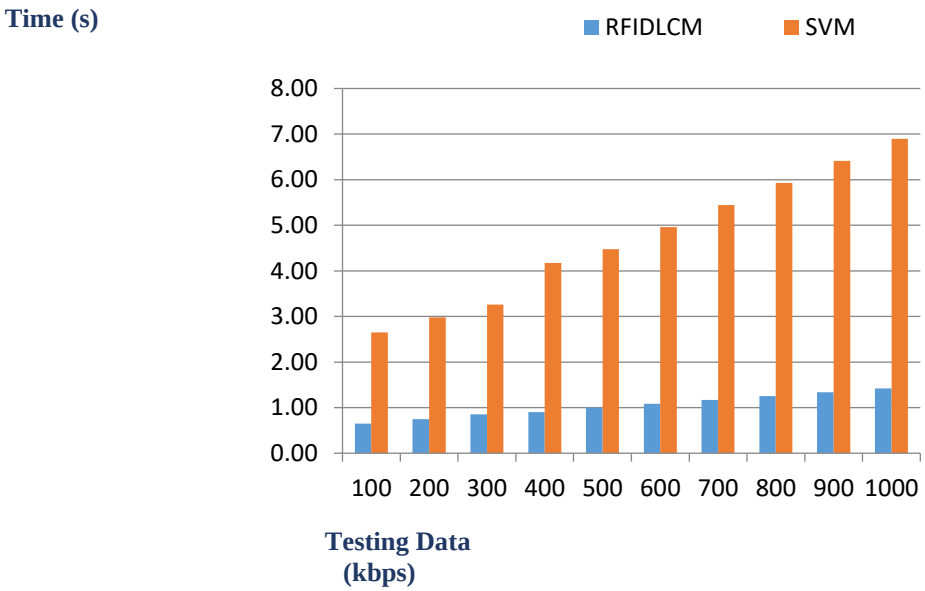


Fig.6 Processing Time Estimation

The following figure, Fig-7 illustrates the data transportation efficiency levels of the proposed approach, in which it shows the accurate measurements of the number of data packets sent from the Smart Health care device and number of data packets received over the remote server.

Fig.7 Data Transportation Efficiency

7.Conclusion and Future Scope

To provide a structure for health care monitoring system implementation, the device aims to perform a survey of current IoT technology. It could be seen that wireless technology choices that deal with IoT enabled health care monitoring system device deployment are extremely broad. Since IoT is a fashionable technology, a multitude of technologies are being built to satisfy all IoT group requirements. In recent years, a number of IoT communications solutions from health care monitoring system have indeed been proposed to connect network system that can recognize and accumulate valuable knowledge. RFID methodology plays a crucial role as a central internet technology. In the international context, increasingly related data on privacy will be created in the context of increasing medical technology, and the protection of the RFID technology in the medical setting has

been increasingly taken into account. Using the RFID scheme to the medical sector, medical privacy information can be managed conveniently and securely. We present in this framework a lightweight shared authentication protection framework that could be applied in mobile medical fields. Medical data is important for users or properties, and the accuracy and synchronization of user credentials is guaranteed in this scheme. It can also avoid the usual attacks. It is important to note that self identity information is of great importance in the medical environment and is closely linked to patient privacy and the proposed scheme guarantees the confidentiality of the tag, in accordance with the medical system's security requirements. This protocol also uses the creative index community to store authentication data that is easy to find and retrieve. Next, we will continue to concentrate on RFID mechanisms over the medical industry and optimize protocol usage in communication efficiency.

In future the proposed work can further be enhanced by means of adding some deep learning strategies to improve the efficiency of the proposed approach with powerful disease predictions over less time period.

References

1. Mostafa Haghi, Sebastian Neubert, Andre Geissler, Heidi Fleischer, Norbert Stoll, Regina Stoll and Kerstin Thurow, "A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring", IEEE Internet of Things Journal, 2020.
2. Adarsh Kumar, Rajalakshmi Krishnamurthi, Anand Nayyar, Kriti Sharma, Vinay Grover and Eklas Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes", IEEE Access, 2020.
3. Tejasvi Alladi, Vinay Chamola and Naren, "HARCI: A Two-Way Authentication Protocol for Three Entity Healthcare IoT Networks", IEEE Journal on Selected Areas in Communications, 2020.
4. Prasenjit Chanak and Indrajit Banerjee, "Congestion Free Routing Mechanism for IoT-Enabled Wireless Sensor Networks for Smart Healthcare Applications", IEEE Transactions on Consumer Electronics, 2020.
5. Gagangeet Singh Aujla and Anish Jindal, "A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring", IEEE Journal on Selected Areas in Communications, 2020.
6. Taiyang Wu, Fan Wu, Chunkai Qiu, Jean-Michel Redouté and Mehmet Rasit Yuce, "A Rigid-Flex Wearable Health Monitoring Sensor Patch for IoT-Connected Healthcare Applications", IEEE Internet of Things Journal, 2020.
7. Partha Pratim Ray, Neeraj Kumar and Dinesh Dash, "BLWN: Blockchain-Based Lightweight Simplified Payment Verification in IoT-Assisted e-Healthcare", IEEE Systems Journal, 2020.
8. Po Yang, Dainius Stankevicius, Vaidotas Marozas, Zhikun Deng, Enjie Liu, Arunas Lukosevicius, Feng Dong and Lida Xu, "Lifelogging Data Validation Model for Internet of Things Enabled Personalized Healthcare", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020
9. Anar A. Hady, Ali Ghubaish, Tara Salman, Devrim Unal and Raj Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study", IEEE Access, 2020.
10. Eman M. Abou-Nassar, Abdullah M. Iliyasu, Passent M. El-Kafrawy, Oh-Young Song, Ali Kashif Bashir et al., "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems", IEEE Access, 2020.