INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

RACSIT - 17

SURVEY ON DESIGN OF PATIENT BLOOD PRESSURE MONITORING SYSTEM USING SECURE IOT

Meghana K M [*1], Manjunath C R [2]
[*1] 4th Semester CSE, M.Tech. Student, SET, Jain University, Bengaluru, India
[2] Associate Professor, SET, Jain University, Bengaluru, India

DOI: https://doi.org/10.29121/granthaalayah.v5.i4RACSIT.2017.3359

Abstract

Blood Pressure Monitoring using sensor and cloud technology, Personal biological readings such as blood pressure are collected by sensor networks device from patients at homes and will be transmitted to cloud and get treated accordingly. It is very important that privacy of patient's medical condition is protected while data are being transmitted over the public network as well as when they are stored in servers. In this paper, a unique Cryptography technique has been used, Cryptography allows privacy of data that is transmitted. This will ensure that it is implemented for small foot print using IOT for secure data transmission. While data is transmitting to cloud Doctor will get email/message notification and Doctor can also view the Patient Blood Pressure Record stored in cloud.

Keywords: Blood Pressure; IOT; Cloud Computing; Encryption; Decryption.

Cite This Article: Meghana K M, and Manjunath C R. (2017). "SURVEY ON DESIGN OF PATIENT BLOOD PRESSURE MONITORING SYSTEM USING SECURE IOT." *International Journal of Research - Granthaalayah*, 5(4) RACSIT, 86-90. https://doi.org/10.29121/granthaalayah.v5.i4RACSIT.2017.3359.

1. Introduction

The Blood Pressure, a critical physiological parameter of the human body, is also a vital indicator in clinical care and even in the daily health care. In the modern society with rich material lives, high blood rate is continuously increasing. In the meantime, individuals connect increasingly significance to their wellbeing and expectation that they can know their wellbeing conditions whenever for averting different illnesses. Consequently, sheltered and easy to-utilize Blood Pressure Monitoring screens get to be distinctly regular home pulse measuring devices [1]. Presently, two normal kinds of blood pressure monitors in the market are mercury column blood pressure strain gage and electronic blood pressure monitor. This paper focuses on electronic Blood Pressure Monitor. With the development of new modern medical equipment, intelligent medical treatment becomes a more trend. Depending on the Internet of things, it is a health care

information platform that accomplishes cooperation between patients, therapeutic faculty, medicinal establishments and restorative gadgets over a remote system. The fundamental thought of the plan is collecting client's/user's vital signs information by utilizing sensors like vital signs detection equipment, then exchanging the information over a remote system to a remote administration stage. After this, the server farm on the stage will do the near investigation of the information. In the interim, as per the information markers, the specialist will furnish remote clients with restorative treatment and wellbeing administration [1]. With the ceaseless improvement of keen medicinal treatment, more shrewd wellbeing checking items will proceed to develop, and this exploration is to cater for this open door.

Cloud computing permits clients to get to programming applications and registering abilities, while utilizing distinctive administration models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2]. These three administration models are depicted beneath:

- Infrastructure as a Service (IaaS) empowers the consumer/customer to give major registering assets, (for example, storage, processing, networks and so on.). The customer can send and also can deploy and run various types of programming and software including working frameworks and systems.
- Platform as a Service (PaaS): This model empowers the customer to send onto the cloud infrastructure applications made or procured by the customer.
- Software as a Service (SaaS): In this model, the client can profit of the capacity of utilizing applications as of now conveyed on the cloud condition by a provider.

Keeping in mind the end goal to give a novel system that upgrades information security in the cloud computing condition, this paper examined cryptographic algorithms helpful to encode information outsourced to cloud storage.

This paper is further divided into following sections. Section II discusses cryptography algorithm with encryption process and Basic Terminology used in Cryptography encryption terminology. In section III present Methodology. Section IV contains Conclusion and References are included in Section V.

2. Cryptography Algorithm

Cryptography is the investigation of Secret (crypto-) and Writing (- graphy), individually [3]. It's a strategy for securing and transmitting data or message in a particular edge so that those for whom it is proposed can read the data and process it. In Modern PC innovation, cryptography is much of the time associated with scrambling typical substance (in like manner implied as plaintext) changed over to Cipher content/message, the methodology returned to encryption then again plaintext, the strategy known as decryption.

Current cryptography frets about four targets, for example, Confidentiality (the information can't be grasped by anyone for whom it was unintended), Integrity (the information can't be altered or recognized or can't be changed or perceived), Non-repudiation (the sender of the information can't deny at a later stage their objectives in the creation or transmission of the information), and

Authentication (the sender who sending information and recipient who gets information can affirm each other's personality/identity and the destination of the data).

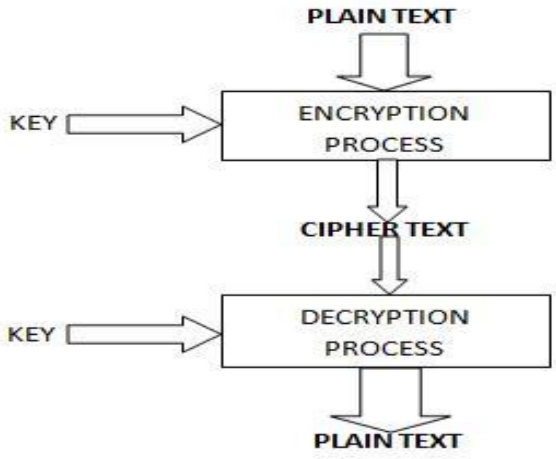

Figure 1: Encryption Process

There are various algorithms for performing encryption and decryption. The most and best fruitful algorithm utilize a key. A key is just a parameter to the calculation that permits the encryption and decryption procedure to happen. The present field of key-based cryptography algorithm can be isolated into two sorts, for example, symmetric-key cryptography and asymmetric cryptography/ Public-key cryptography. Symmetric-key cryptography alludes to encryption systems in which both the sender who sends the data and recipient who receives the data have a comparative key. The public-key cryptography will be Cryptography in which a few keys is used to encode & decode a message with the objective that it arrives safely & securely. Asymmetric encryption gives more prominent security when contrasted and symmetric key encryption however in case of encryption speed, symmetric encryption is on lead [4]. Another Cryptography algorithm is Cryptographic hash work/function that changes over a numerical info esteem/value into another compacted numerical esteem/value and that uses a Mathematical change to irreversibly "encrypt" the information.

Basic Terminology used as a piece of Cryptography

There are few terms which we ought to know for better comprehension of encryption calculations. This phrasing is vital to comprehend on the grounds that in each algorithm description, we will discuss these consistent terms:

1) **Plain Text or Normal Text:** The first message or content utilized as a part of correspondence is called as Plain content. Illustration: Alice sends "Hello" to Bob. Here "Hello" is Plain content or Original message.
2) **Cipher Text:** The plain content is encoded in un-intelligible /un-readable message. This negligible message is called Cipher Text. [5]
3) **Encryption:** Encryption is a procedure of changing over Plain content into Cipher content. This non-lucid message can safely be conveyed over the unsecure network. Encryption process is done utilizing encryption algorithm.

4) **Decryption:** process is the switch of Encryption process, i.e. Cipher content is changed over into plain content utilizing specific encryption algorithm.
5) **Key:** A key is an Alpha-numeric or numeric substance (scientific recipe/mathematical formula). In encryption it occurs on Plain content and in decryption it occurs on cipher content.
6) **Key Size:** Key size is the measure of length of key in bits, used as a piece of any algorithm.
7) **Block Size:** Key cipher takes a shot at settled length series of bits. This settle length of string in bits is called Block measure. This piece measure depends algorithm.
8) **Round:** of encryption implies that how much time encryption capacity is executed in entire encryption prepare till it gives cipher message as yield [4].

3. Methodology

In this fragment, we give an intelligible delineation of the approach proposed to countermeasure data security issues in cloud computing.

Respond in due order regarding enhancing data security in the cloud: While using cloud/distributed storage, sharing resources, especially sharing data between data proprietor and endorsed clients, can speak to the threat of data break or spillage. Honestly, securing data in the cloud is difficult to fulfill if the client trusts the specialist co-op. The client is obliged to heedlessly trust the supplier's frameworks yet this can be keep around the perils of vindictive insiders among them cloud administrators who can get to data fundamentally.

To guarantee information security, numerous strategies and advancements are proposed so in those the most effective one is cryptography. The best approach received to secure information is symmetric cryptographic systems. Be that as it may, this method alone is not productive in a multi-occupant situation; many approved customers have the privilege to get to information so the key must be circulated to every customer. The key administration is excessively troublesome, making it impossible to do that task are dangers in sending keys to various customers in the meantime. The asymmetric cryptographic procedures is an appropriate approach to guarantee information security. Despite the fact that, this arrangement limits information access to the information proprietor which negates the multi-clients part of cloud computing. In addition, the unbalanced cryptography calculation shows an overwhelming effect on information get to.

This more often than not doesn’t permit the encryption of an information in worthy time for clients. Hence, it is important to execute & propose another arrangement that can offer an exchange off between the security prerequisites & framework execution and which saves the multi-tenure part of cloud computing [2].

1) **Existing System:** We are considering Digital BP monitor is which totally Automatic Upper Arm Blood Pressure Monitoring device, gives Comfortable, Quick and Accurate Blood Pressure Monitoring. This device does not have any Cloud connectivity with Data Security and doctor notification.

2) **Proposed System:** The technology enables monitoring of patients' blood pressure using digital technologies to collect data from individuals and electronically transmit that information securely by cryptography mechanism to Cloud service simultaneously notify doctor with email/alert message which is low cost, fast By incorporating IoT worldview into these frameworks can additionally expand knowledge, adaptability and interoperability. A gadget using the IoT plan is remarkably tended to and identifiable at whenever and anyplace through the Internet for further evaluation and suggestions.

4. Conclusion

Sensor cloud technology enables the early detection of adverse conditions and diseases. My purpose is to work on technology to provide additional features such as encryption and encryption of Patients data while transferring to cloud which allows privacy of data that is transmitted with Email/Alert message to doctor and to develop an interactive application which collects all the necessary details from the patients which helps doctors to analyze data without physical presence.

References

[1] Lekai Zhang, Jiaxi Wang, Baixi Xing, Shouqian Sun, Zenggui Gao , Kejun Zhang, Smart Blood Pressure Monitoring System Based on Internet of Things. April 27 – May 2, 2013, Paris, France.
[2] Sana Belguith, Abderrazak Jemai, Rabah Attia, Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm. ICAS 2015: The Eleventh International Conference on Autonomic and Autonomous Systems.
[3] Rahman MM*, Akter T and Rahman A, Development of Cryptography-Based Secure Messaging System, Rahman et al., J Telecommun Syst Manage 2016.
[4] Rajdeep Bhanot, and Rahul Hans, A Review and Comparative Analysis of Various Encryption Algorithms, International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306.
[5] International Journal of Security and Its Applications Vol. 9, No. 4 (2015) Copyright ⓒ 2015 SERSC 291 Example: "Hello" message is converted in this meaningless message is Cipher Text.

*Corresponding author.
E-mail address: meghanakm22@gmail.com