How to Cite:
Govindaraj, M., Murugeswari, P., Bharathiraja, N., Thiagarajan, R., Ahamed, I. S. B., & Manikandan, T. (2022). Evolution of IOT in health care by protecting and safeguarding private security in healthcare. *International Journal of Health Sciences*, *6*(S6), 5912–5920. https://doi.org/10.53730/ijhs.v6nS6.11133

Evolution of IOT in health care by protecting and safeguarding private security in healthcare

Govindaraj M.
Sr. Assistant Professor, Department of MCA, New Horizon College of Engineering, Bangalore
Email: govindaraju.mca@gmail.com

Dr. P. Murugeswari
Professor, Department of CSE (Cyber Security), Karpagam College of Engineering, Coimbatore
Email: pmurugeswarik7@gmail.com

Dr. N. Bharathiraja
Associate Professor, Dept of ECE, Veltech Multitech Engineering College Avadi, Chennai
Email: bharathinatarajan78@gmail.com

Dr. R. Thiagarajan
Associate Professor, Dept of IT, Prathyusha Engineering College, Chennai
Email: rthiyagarajantpt@gmail.com

Inayath Ahamed S. B.
Assistant professor, Kalasalingam business school, Kalasalingam academy of research and education (deemed to be university), Krishnankoil
Email: inayathahamed@klu.ac.in

Dr. T. Manikandan
Professor, Department of Electronics and Communication Engineering, Rajalakshmi Engineering College, Thandalam, Chennai
Email: manikandan.t@rajalakshmi.edu.in

Abstract---Machines are being linked together in order to lessen the burden of medics in the near future while also offering effective services to patients. Furthermore, these gadgets generate a large amount of data during transmission. A clinical IoT based network is a networked system that must be protected from beginning to finish in order to function and communicate. To avoid sensitive data leakage from such devices/systems, connection should be encrypted. We are proposing dynamic encryption model which works well on health

records generated from IoT machines. Similarly, we ensure the security of the data through a two-way authentication system with the approval from agent/patient to access and share the data.

Keywords---IoT, dynamic encryption, two-way authentication approach.

Introduction

Big Data is being created as a result of recent advancements in smart/electronic gadgets or computer systems. In layman's terms, this data is referred to as "Huge Datasets" or "Big Data." After a thorough and comprehensive study, today's Big Data is extremely beneficial for forecasting the future. Several academics have attempted to create efficient analytics techniques to evaluate this health care Large Data, however some methods have failed owing to the amount and veracity of the big Data. As a result, various problems, issues, and difficulties have been resolved that must be faced in the near future. As a result, the proposed study provides insight into how and where health care big data might be employed in the health care system, as well as various problems and opportunities.

Because of the volume of data, the variety of data types, and the speed with which it can be managed, big data in healthcare is crucial. It should be noted that the data used for e-healthcare applications includes clinical data (prescription, insurance, and pharmacy), patient data, machine generated/sensor data, and less patient oriented data. Some advantages of big data/genomic analytics in e-health care are: Disease detection at an earlier stage, Disease prevention, Identifying health-care fraud. Predicting: individuals who will choose surgery, who will not benefit from surgical intervention, odds of disease progression, and so forth. So, there will be enormous data collected over every procedure but to preserve the data with security and integrity is the challenge. It is obvious that patient protection and data security is a major worry within the industry, but rising costs and an ever-growing consideration with organisations ability to protect against breaches has recently come to light. providers are required to inform patients any time there will be a breach of "unsecured" patient health information Encryption has become the most important practise as healthcare data migrates rapidly into the digital sphere. The components presented are being developed as part of the proposed model.

The design provides for the monitoring of both acute and non-chronic individuals, as well as healthy persons who require monitoring due to various conditions in both the home and the external world. Furthermore, it enables engagement with their family, emergency services, and hospitals through the use of Cloud technology, Big Data, and Smart devices techniques. IoT plays an important part in our design, allowing users to benefit from the use of various wearables and sensor devices. The design includes the following essential aspects: smart mobiles that accept data from portable wearables, vital signs sensors, a cloud-based infrastructure for data storage and an analytic component for authentication of alarms to be sent to the person and/or patient's caregivers, access to different cloud manufacturers' sensors, and an integration and messaging platform for

knowledge dissemination to all involved parties. The IoT based privacy preserving model consists of a two-way authentication system for the patients and the health care provider. The IoT devices connected to the cloud will initiate the secure key value form the network for data access. The patient as well as the health care provider has to generate the verification code in which the health care provider can also automatically generate the same. We do provide a framework for alerting the admin on the suspicious log on, security breaches on the mobile itself to provide protection from the hacks.

Literature Review

S. K. B V, [1] introduced a paper on IoT can be useful in medical and medical centres because it enables detailed investigation of degenerative illnesses, critical indicator tracking, crisis detection, diagnostics, and predictive modeling. The Iot becomes apparent and beneficial in the healthcare setting and elderly care, i.e., tasks that need the complete participation of a caregiver or medical worker in most circumstances. The goal of this study is to provide insight on the relevance and types of IoT-enabled adult treatment and rehabilitation. This publication compiles a review of studies on the creation and implementation of IoT-enabled adult medical services. The article discusses several IoT-based strategies that may be utilised for smart healthcare.G.S [2] proposed a paper on, a Remote Healthcare Monitoring System was developed using wearable health devices and a microprocessor. The monitoring system provides, displays, and stores the patient's core temperature, ECGM, heart rate, and oxygen levels in plasma (SpO2). These data are transmitted to the website via the Arduino Ethernet Shields, which are accessible to health care providers as well. Mortality from cardiac disorders and medical conditions caused by an irregular heart rate are now on the rise. Because of the current epidemic crisis, it is exceptionally hard for a patient to approach a hospital or clinical facility. This technology helps the physician to watch the patient's condition from the comfort of their home, as well as evaluate the health information, give medical support, and propose medications.

According to Alladi [3], Various authenticating methods have emerged recently to solve these difficulties, but the security measures of health IoT systems from node manipulation and node substitution threats, in particular, aren't fully resolved in the research. To solve those problems, this work presents two authentication mechanisms based on dedicated hardware components known as Physically Unclonable Functions (PUFs). Considering the storage and energy limits of medical IoT systems, this framework is intended to be very lightweight. A stringent safety examination is performed to demonstrate the system's correctness. In respect of computing speed and security, we also contrast it to comparable methods in the e-healthcare situation to demonstrate its applicability and resilience. Sadek, [4] introduced a paper where those end users grant authorization to highly vulnerable or leaky third-party applications, they open themselves up to malicious attacks. Because the data is stored on the cloud, it travels over unsecured methods of communication, both of which raise security concerns. Furthermore, there really are additional data security risks whenever the data is projected into the proprietor's internet storage unit.

We describe a few of the available IoT sleeping monitors throughout this research, as well as highlight the most prevalent aspects related to all these sleeping monitors. because the great majority of end users are unaware of the privacy-related risks associated with new IoT sleep monitors. We look at current solutions that could be used for the structure of an IoT sleep timer. We additionally explain a deployable Internet of Things system which can handle these challenges. According to Panchatcharam [5] due to a lack of facilities, India is dealing with a slew of medical issues. This study article illustrates the concept of resolving health difficulties with the use of a new breakthrough, the Iot. The Internet of Things, with its growing transdisciplinary uses, has revolutionised our lives. However, one IoT platform is smart affordable healthcare, which connects clever devices, equipment, doctors, professionals, and monitors to the internet. Finally, the challenges and potential for the advancement of Internet-of-things medical service systems are discussed in depth. This evaluation furthermore outlines IoT security concerns, IoT services and apps, and innovative health services that have modified the traditional medicinal setup by making affordable healthcare management more efficient via their apps.

Methodology

Starting with the security and privacy needs of the medical IoT technology, this system analyses security and privacy concerns from a technological standpoint and provides future research problems. The system discusses on two major areas of works such as two-way authentication framework, cloud-based data storage and a multi-level encryption mechanism for the same. Automatic message dissemination mechanism to the admin on data breach/theft on the network in the IoT based networks. Cloud services are mostly used for distributed data gathering, processing, aggregation, and analysis on that data. This information is received by sensors that are delivered as a service. The fundamental components of IoT are connected devices, which gather data and communicate with other devices/humans. To safeguard security and privacy, confidentiality, and comfort so that we may really reap the potential of the Internet of Things using multi-level encryption mechanism. Planning low-cost solution and prevent phishing, denial of service, brute-force assaults, and network injections are all examples of man-in-the-middle attacks using an automatic message delivery on the admin. Authentication from admin/patient for data sharing are carried out.

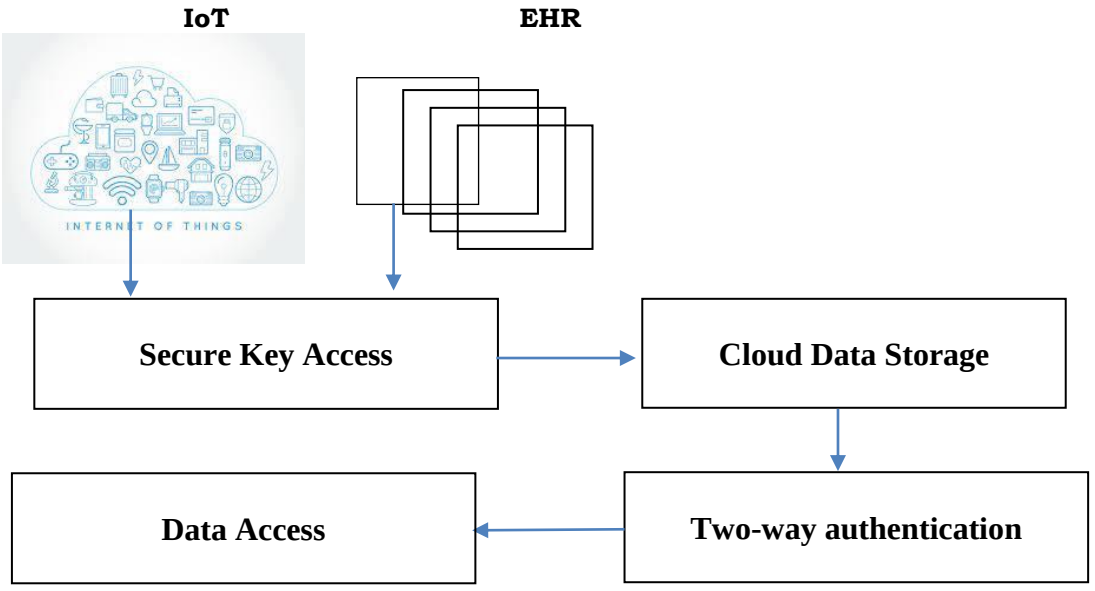

Figure 1. Architecture Diagram

Construction
IoT

Physicians may keep records of patients' health more efficiently by employing wearable as well as other residential monitoring devices connected to IoT. Clinicians can monitor patients' medication compliance regimens and identify any in need of rapid hospital treatment. IoT helps health providers to become more vigilant and reactive in their patient interactions. Incoming data from IoT systems can assist clinicians in determining the appropriate treatment approach for patients and achieving the desired results. Since communications between physicians have gotten simpler and more convenient, the IoT has enhanced patient involvement and satisfaction. Moreover, monitoring equipment of a patient's condition indirectly improves hospitalizations and avoids re-admissions. The IoT has a huge influence on lowering medical costs and increasing therapeutic outcomes. Physicians may keep records of patients' health more efficiently by employing wearable as well as other home monitoring systems connected to IoT. Clinicians can monitor patients' compliance with treatment regimens as well as any need for rapid medical assistance. IoT helps health providers to be more vigilant and proactive in their interactions with patients. Data received from IoT devices can assist clinicians in determining the appropriate treatment method for patients and achieving the desired objectives.

HER

IoT-based health services are not made to handle or avoid infiltration, opening them up to assaults including such malware, wherein attackers target the network using software that provides security and prohibits hospital and healthcare users from sharing EHRs and datasets. Patients' physiological signals could be collected remotely and stored in an Ehr System (EHR). Furthermore, a

common network amongst health practitioner's aids in the diagnosis, analysis, and resolution of patients' issues. In terms of being able to remotely watch patients, physicians may also track their vital signs. An EHR is susceptible to attackers and it is challenging to distribute between multiple health institutions when required while jeopardising patient confidentiality. The suggested IoT-based solution protects patient EHR administration to prevent unwanted access and modification. To safeguard the critical data stored in the database, encrypting strategies are employed. Initially, the Internet of Things (IoT) and health in IoT were presented. Apart from the privacy-related considerations that influence EHR. Then we showed a structure in which we safeguard patients' EHRs and impose authorization limitations. The physician must connect to the system to register the patient's Ehr systems in the system, and he or she must present their credentials to the system for identification.

Secure Key Access

An app may have several users, each with varying levels of authorised access. A reliable identity management method is necessary at the application level. To maintain information safety here on the cloud, this must be protected against intrusions. It may be accomplished by employing tools for identifying cloud movement of data, data backup technologies, and files or relational continuous monitoring. Information dispersal and segmentation can be used to secure information in the cloud. Node identification is needed to avoid unauthorised system access. Because security and anonymity of data to also be communicated among nodes are critical, light-weight encryption methods must be created to reliably communicate data over the network. Access control is another issue that must be addressed in the setting of IoT devices.

Cloud Data Storage

The usage of cloud resources in conjunction with IoT enables quick gathering, evaluation, and deployment of assistance and solutions. This allows for telehealth and protects clinical staff against getting into close touch with patients in a potentially contaminated and dangerous workplace environment. Cloud hosting is a public cloud concept in which data is stored on the Web by a public cloud provider that maintains and administers information software as a service. As smart sensors collect, transmit, and store health information, it allows data insights and digital medical services that might enhance health risk recognition, illness diagnosis, therapy, and telemonitoring, as well as empower people to identify. Cloud IoT technology has been widely used in remote health surveillance and provides viable solutions for individuals suffering from significant health problems and impairments. Monitoring through Virtualized and IoT assists in the preventive and early diagnosis of illnesses, and as a result, appropriate healthcare treatments may be supplied to ensure patient ease and safety. Because of the minimal cost and accessibility of sensing, cloud-based Iot e-based applications have greatly increased in recent years. There are a variety of implanted and peripheral sensing devices on the marketplace today that provide specific and reliable monitoring. Several additional uses, particularly healthcare, create massive amounts of data that need legitimate analytics. This, therefore, necessitates a dynamic network design to support the enormous traffic volume

created by diverse devices. IoT additionally comes with restricted network bandwidth, which significantly reduces its efficiency. Previously, sensors typically sent data to centralised servers that had enough computational infrastructure and services.

Experimental Results

Two-Way Authentication Approach

Because disclosing a patient's health information is improper, any information captured from an ecosystem must be stored securely. To secure the information of IoT health records, all user devices involved should be verified. It is critical that the patient's identification as well as the devices be correctly handled. As a result, device identification and permission of access to medical care data are critical difficulties during an Internet-of-things health service. Usually, a unique credential method is used for access control authorisation to IoT devices. However, such techniques are frequently subject to exploitation. To preserve battery power, the patient nodes don't really retain a constant connection with a wirelessly mobile sink; rather, they run in turbulence phases. When it wakes up, it must first create a secure authorised connection with the wireless sensor nodes, collect data from every clinical sensor attached to it, transfer this to the wirelessly mobile sink, and go back to sleep state for a predefined amount of time. A user attempting to access an end device must first verify its device. Only then can a secure communication link to such a device be created. Aside from identification, the encrypted data provides further safety.

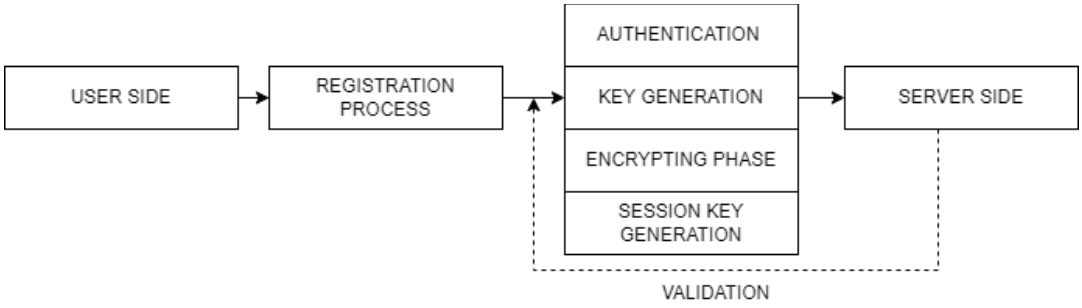

Figure 2. Authentication Approach Process

Conclusion

The fundamental components of IoT are connected devices, which gather data and communicate with other devices/humans. To safeguard security and privacy, confidentiality, and comfort so that we may really reap the potential of the Internet of Things using multi-level encryption mechanism. Planning low-cost solution and to prevent phishing, denial of service, brute-force assaults, and network injections are all examples of man-in-the-middle attacks using a automatic message delivery on the admin. Authentication from admin/patient for data sharing. Communications must be protected to protect sensitive information leaking from certain components. We propose an adaptive encryption scheme that performs well together with medical files collected from IoT devices. Furthermore,

we secure data protection with a two-way authentication mechanism that requires physician/patient authorization to view and exchange data.

References

1. Srilakshmi, P. Mohanapriya, D. Harini and K. Geetha, "IoT based Smart Health Care System to Prevent Security Attacks in SDN," 2019 Fifth International Conference on Electrical Energy Systems (ICEES), 2019, pp. 1-7, doi: 10.1109/ICEES.2019.8719236.
2. Alladi, Tejasvi & Naren, Naren & Chamola, Vinay. (2020). HARCI: A Two-Way Authentication Protocol for Three Entity Healthcare IoT Networks. IEEE Journal on Selected Areas in Communications. 10.1109/JSAC.2020.3020605.
3. G. S, V. L, R. V. B, D. SS and A. N, "IoT Based Health Monitoring System," 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 2021, pp. 1-6, doi: 10.1109/i-PACT52855.2021.9696937.
4. Ibrahim Sadek, Shafiq Ul Rehman, Josué Codjo, and Bessam Abdulrazak. 2019. Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations. In How AI Impacts Urban Living and Public Health: 17th International Conference, ICOST 2019, New York City, NY, USA, October 14-16, 2019, Proceedings. Springer-Verlag, Berlin, Heidelberg, 3–17. https://doi.org/10.1007/978-3-030-32785-9_1
5. Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. Acta Inform Med. 2019 Dec;27(4):253-258. doi: 10.5455/aim.2019.27.253-258. PMID: 32055092; PMCID: PMC7004290.
6. Panchatcharam, Parthasarathy & Sundaram, Vivekanandan. (2019). Internet of Things (IOT) in Healthcare – Smart Health and Surveillance, Architectures, Security Analysis and Data Transfer: A Review. International Journal of Software Innovation. 7. 21-40. 10.4018/IJSI.2019040103.
7. R.Thiagarajan, R.Jothikumar,T.Rubeshkumar,P.Jayalakshmi,M.Baskar“Enhanced Resemblance Measures forIntegration in Image-Rich Information Networks”, Journal of Critical Reviews,ISSN- 2394-5125 Vol 7, Issue 16, July 2020
8. R.Thiagarajan,N.R .Rajalakshmi , M. Baskar ,P. Jayalakshmi “A Novel Solution for Economizing Water by a Mix of Technologies with a Low Cost Approach”, International Journal of Advanced Science and Technology Vol. 29, No. 7, April 2020, pp. 916 – 921.
9. S. A. Chaudhry, K. Yahya, F. Al-Turjman and M. -H. Yang, "A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems," in IEEE Access, vol. 8, pp. 139244-139254, 2020, doi: 10.1109/ACCESS.2020.3012121.
10. S. K. B V, S. Sharma, K. S. Swathi, K. R. Yamini, C. P. Kiran and K. Chandrika, "Review on IoT based Healthcare systems," 2022 International Conference on Advanced Computing Technologies and Applications (ICACTA), 2022, pp. 1-5, doi: 10.1109/ICACTA54488.2022.9753547.
11. S. Sonune, D. Kalbande, A. Yeole and S. Oak, "Issues in IoT healthcare platforms: A critical study and review," 2017 International Conference on Intelligent Computing and Control (I2C2), 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321898.

12. Sadek, Ibrahim & Rehman, Shafiq & Codjo, Josué & Abdulrazak, Bessam. (2019). Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations. 10.1007/978-3-030-32785-9_1.
13. Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2022). Post-pandemic health and its sustainability: Educational situation. *International Journal of Health Sciences*, *6*(1), i-v. https://doi.org/10.53730/ijhs.v6n1.5949
14. Susilo, C. B., Jayanto, I., & Kusumawaty, I. (2021). Understanding digital technology trends in healthcare and preventive strategy. International Journal of Health & Medical Sciences, 4(3), 347-354. https://doi.org/10.31295/ijhms.v4n3.1769
15. T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 819-824, doi: 10.1109/TrustCom/BigDataSE.2018.00117.
16. V. Vippalapalli and S. Ananthula, "Internet of things (IoT) based smart health care system," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 1229-1233, doi: 10.1109/SCOPES.2016.7955637.
17. Villalba, M. Teresa & Buenaga, Manuel & Gachet, Diego & Galisteo, Fernando. (2015). Security analysis of an IoT architecture for healthcare.