IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SECURITY OF IoT IN THE CONTEXT OF E-HEALTH AND CLOUD

[1]**Dr A. Rajasekaran**,[1]Assistant Professor, Dept of ECE, SCSVMV University, Enathur, Kanchipuram. arajasekaran@kanchiuniv.ac.in

[2]**Mr Nishanth Kiruthivasan**,[2]UG scholar, Dept of ECE, SCSVMV University, Enathur, Kanchipuram.
nishvask@gmail.com

[3]**Mr Nittala Datta Pavan Kumar**,[3]UG scholar, Dept of ECE, SCSVMV University, Enathur, Kanchipuram.
dattanittala0606@gmail.com

**Abstract— Devices are now vulnerable because of Internet of Things (IoT) and cloud technologies. The many dispersed devices may gather, store, and analyze data in novel ways as they transfer real-time information to open, private, or hybrid clouds. Depending on the security and privacy of the IoT devices, the rising deployment of IoT devices in the healthcare setting exposes patient information to hostile assaults. There is regrettably a lack of a comprehensive examination of the security difficulties in the IoT for e-Health on clouds, even though many academics have investigated such security concerns and open questions in IoT. We attempt to close this gap in this study by undertaking a detailed examination of IoT security flaws. We then discuss current methods that have been offered to address security issues in the cloud for the e-Health area. We also provide a proposal for a cloud based IoT solution.**

**Keywords—IoT; CLOUD; E-HEALTH; SECURITY.**

## I. INTRODUCTION

One of the main areas of study is on improving healthcare services and peoples' quality of life. E-health systems are a more recent work for healthcare practices based on software and communication technologies.

The next generation enables the development of IoT and cloud computing services by integrating information, people, devices, and context.

The usage of cloud computing in healthcare can have certain advantages for patients as well as for hospitals and other healthcare facilities. These days, cutting costs is very essential, and the ability of doctor and hospital collaboration utilizing cloud computing networks might boost the quality of care.

The EUROPEAN COMMISSION INFORMATION SOCIETY defines the Internet of Things (IoT). Personal computers, sensors, tablets, smartphones, and other embedded systems are examples of IoT devices. the Internet of Things the extensive network of devices linked to the Internet, which includes smart phones, tablets, and nearly anything with a sensor - including automobiles, machinery in manufacturing facilities, jet engines, oil drills, wearable technology, and more. These "objects" share and gather data.

IoT and the machine-to-machine (M2M) technology that powers it are giving almost every industry a form of "super visibility." Imagine a world when utilities, telecommunications companies, and airlines can all forecast and prevent failures, optimize jet performance, and base treatment decisions on real-time genomic analysis. There are countless commercial opportunities.

IoT refers to several devices being connected to one another in a conceptual sense, allowing for the collection of real-time data and the analysis of that data. The detected data is processed at a node, where linked devices observe their surroundings and ascertain what is happening. This information is gathered to allow devices to make decisions on their own or to inform users so they can make the best judgments.

IoT and cloud technologies are interdependent. IoT opens the door to reducing technology limitations including those related to storage, processing, and energy. The cloud is a technology that is now available and providing additional services. However, there are issues with security and privacy when combining cloud services with IoT. The integrated cloud environment should maintain the privacy and security of the data.

To safeguard medical data without sacrificing the effectiveness of services in the E-health environment, Cloud and IoT technologies implemented as a component of medical information systems must meet certain critical security standards including integrity, confidentiality, availability, and authentication.

## II. IoT AND CLOUD: OPPORTUNITIES AND VULNERABILITY IN E-HEALTH CONTEXT:

### A. IoT and CLOUD opportunities in healthcare:

Integration of cloud computing with IoT enables new networking, processing, scalability, and storage capabilities that are crucial for creating and sustaining connected, intelligent, and customized healthcare services. The capacity of auto-configuration, interoperability, self-management, intelligent interaction with other objects, and initiation of processes based on data and context increases medical staff's decision-making while also increasing the efficiency and effectiveness of the care process.
We'll now outline the rationale for its application in e-health. Utilizing this approach, several issues, including integration costs and resource optimization in new age innovation, have been resolved. Hospitals and healthcare organizations are storing more electronic data in systems because of technological advancements. Shifting them to the cloud therefore sounds like a smart idea. However, while moving to the cloud has certain benefits, there are also some hazards associated to internet security and privacy. Adopting the cloud approach greatly reduces the organization's cost.

Additionally, bringing this into the house enhanced quality of life and decreased readmission. MBAN (medical body area network) uses sensors to operate at a minimal cost.

## B. SECURITY REQURIMENTS:

The distribution of health information via the internet and telecommunications to consumers and healthcare professionals.

HIPAA (Health Insurance Portability and Accountability Act) specifies several security rules for the use and disclosure of "protected health information" to safeguard this medical information (PHI)

In relation to electronic PHI, the Security regulation focuses on certain administrative, technological, and physical precautions (EPHI). Any Protected Health Information (PHI) that is electronically stored, accessed, or conveyed is referred to as EPHI. Part of the security rule is the protection of EPHI data against unauthorized access.

The security rule's main goal is to preserve the privacy, accuracy, and accessibility of Electronic Protected Health Information (EPHI).
Therefore, we guarantee that ePHI data is shared only with authorized people and entities. Additionally, the EPHI data was not changed during storage, processing, or transmission. The guarantee of confidentiality states that ePHI data will only be shared with approved individuals or groups. Data storage, processing, and transmission are all protected from unauthorized access. Integrity is the guarantee that ePHI data has not been improperly changed while being stored, processed, or transported. Additionally, each data alteration must be acknowledged, demanded, recorded, validated, and authorized. Data integrity is crucial to HIPAA because it guarantees that we can trust the information when making medical judgments. The goal of availability is to ensure that authorized users may access key ePHI data delivery, storage, and processing services, when necessary, both in regular circumstances and in an emergency.

C. IoT vulnerability in a cloud context:

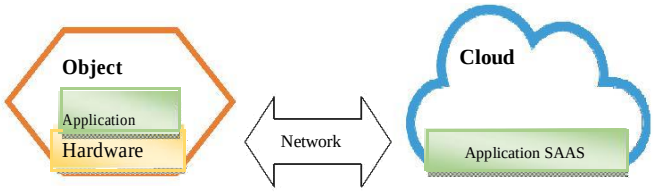



Fig1: Layers of IoT vulnerability in a cloud context

1. Hardware Vulnerability:

From a meteorological and human standpoint perspective, smart devices in the sensing area are anticipated to be protected from physical threats. Common problems with the physical layer include:

- Physical Damage: This vulnerability affects physical objects like sensors, nodes, and actuators that might be physically harmed by intruders or by adverse weather conditions such unusual rain, snow, or wind. This can result in the gadgets' loss of operation and increased vulnerability to dangers.
- Resources constraints: IoT devices have limited resources. These restrictions may relate to the amount of processing power, onboard memory, or energy that is accessible, among other things. When a device runs out of power, it can't really function correctly, which causes a denial of service. IoT embedded systems, which power the devices, may not have enough security modules, and have flimsy network protocol stacks. The functions of IoT devices in a cloud environment depend on the physical resources of the cloud.
- Storage vulnerability: Data may be saved in physical devices and cloud storage thanks to IoT. An Internet of Things (IoT) gadget must be kept secure and private. As a result, inadequate physical protection leaves the storage medium, and data exposed to breaches or unauthorized access.

2. Network Vulnerability:

The vulnerability of the network layer depends primarily on how the integrity and authentication of the data conveyed in the network are respected due to the volume of exchanged data that it carries. Network layer threats frequently include:

- Data Interchange vulnerability: Data transmitted over a network may be the target of gateway or DOS attacks. These assaults can halt data transmission between devices and their source. An excessive amount of data transmitted to the gadget may cause its functions to stop. When network services are discovered to have unused exposed and accessible ports, this may be the situation.
- Unauthorized Access: If suitable authentication mechanisms are not in place, healthcare equipment and systems are vulnerable to several assaults. These attacks include, for instance, impersonation attacks, insider attacks, man-in-the-middle attacks, replay attacks, assaults using stolen verifiers, and password guessing attacks.

3. Application Vulnerability:

The services might be harmed, utilized improperly, or accessed by unauthorized users because of security flaws in the application layer. The following are typical application layer vulnerabilities:

- Cloud applications vulnerability: If IoT applications are hosted on clouds, users may access the devices and apps from any location at any time. This removes access restrictions but also introduces security flaws since these cloud apps might not be secure or might use resources from an unreliable cloud partner.
- Cryptographic vulnerability: IoT devices might not utilize transport encryption or might use rudimentary encryption techniques due to their limited processing capacity. As a result, hostile actors may easily find and track communications. A mobility-sensitive security method must also be developed for IoT devices due to the mobility of these devices.

## III. SECURITY SOLUTIONS FOR IoT IN E-HEALTH CLOUD

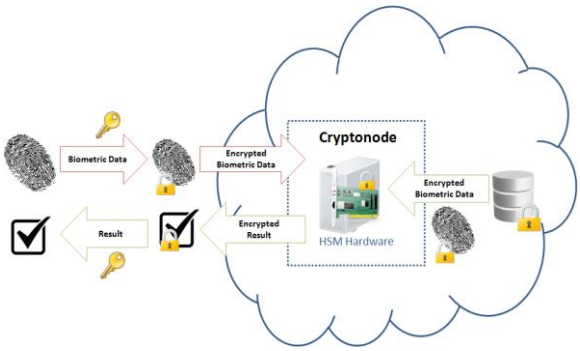
The following are well-known security techniques that have been put out in the literature for IoT that can be applied to a cloud-based e-health domain. To highlight the most recent and successful research-based solutions, these security techniques were chosen from the top publications and conferences.

1. Hardware security solution:
   Instead of using wearable or smartphone sensors to record health parameters, the architecture presented here uses embedded sensors. It communicates quickly and securely using XML webservice.
   Another one is centered on real-time health monitoring, utilizing smart phones to track ECG and other information.
2. Network security solutions:
   Current research on the IoT Cloud platform is concentrated on the architectural design of a system for health monitoring and analysis. For instance, the authors suggest an IoT-Cloud framework employing VIRTUS middleware for e-health systems. It is an XMPP-based publish/subscribe system. To safely transmit data over the internet and prevent data loss in the event of bad connectivity, VIRTUS offers the system an efficient, scalable, and secure communication route.
3. Biometric verification with criptonube:
   Numerous applications for biometric recognition are being developed and are starting to reach the end user. For example, biometrics is a promising replacement for the present methods of authentication and access control, substituting unique user biometric data like fingerprints or iris scans for the conventional username and password credentials. Thus, a person's biometric information is becoming exceedingly sensitive data.

Mobile devices already use biometric technology to verify the user's identity. In this local setting, the user retains control over the biometric data; nevertheless, there are several additional circumstances in which the user must authenticate to insecure environments, such as the cloud.

Data should be given the maximum level of privacy protection in a biometric verification situation in the cloud, such as access to a web service by fingerprint scanning. This option is provided by Criptonube, which executes the biometric verification algorithm within the Secure Hardware Modules of the deployed Cryptonodes in the cloud environment.

Before being delivered to the cloud, biometric data is encrypted on the client side and compared with the encrypted data kept on the database server. Verification and decryption occur just once in the Hardware Secure Module. Criptonube promises that the verification was done in a safe space that was inaccessible to the cloud provider or any other intruders.




## IV. PROPOSED ARCHITECTURE

According to the information presented above, there is still a great deal of room for improving the security of IoT systems within the framework of a cloud-based eHealth system. Most IoT-cloud systems for health care that have been presented are over optimized since they produce a lot of data and continually notify consumers and medical personnel with useless alarms. By enabling the transmission of inaccurate data, IoT device security flaws might harm the cloud ecosystem. We suggest an IoT-cloud based development approach utilizing a bedside cardiac monitor while prioritizing these flaws.

For measurement and therapy, the cardiac monitor is a machine that displays the electrical and pressure waveforms of the cardiovascular system. It is possible to measure parameters unique to respiratory function. The cardiac monitor is maintained by the patient's bedside since electrical connections are formed between it and the patient.

The electrocardiogram (EKG) trace is continually shown on the heart monitor. Cardiovascular pressures and cardiac output may be monitored and presented as needed for patient diagnosis and therapy thanks to additional monitoring components. Bedside monitors, which are most frequently used in emergency rooms and critical care sections, can be integrated to provide continuous monitoring of many patients from a central display. Electrocardiogram, noninvasive blood pressure, intravascular pressures, cardiac output, arterial blood oxygen saturation, and blood temperature are just a few of the parameters that may be evaluated.

Prior to applying the electrode to the skin, a layer of gel that is shielded by a film is removed from the electrode. The right arm, right leg, left arm, left leg, and the centre left side of the chest will all have electrode patches implanted near or on them. For the measurement of a five-lead ECG, the wire will be attached to the electrode patches. Electrocardiograms with three and twelve leads are other variants. A blood pressure cuff will be wrapped around the patient's arm or leg if noninvasive blood pressure measurement is being done. It will be decided whether to inflate the blood pressure cuff manually or automatically. If manual inflation is selected, the cuff will only inflate when the medical professional commands it to, at which point a blood pressure reading will be shown. The blood pressure cuff will inflate at regular intervals during

autonomous operation, and the display will update at the conclusion of each measurement.

In addition to the previously mentioned BEDSIDE CARDIAC MONITOR idea, we also include some secondary security in our suggested design. Here, we are utilizing the transmitter as our ISP, and we purchase our static IP from companies like BSNL.


The patient cannot be examined by the doctor all day. Typically, a bedside cardiac monitor will show blood pressure, pulse rate, and heart rate. In this case, information about the related patient can be obtained through transmitter from the bedside cardiac monitor to the cloud storage. ISP is used by the transmitter to distribute and store this data in the cloud. The receiver retrieves this information and sends it to the appropriate physicians, nurses, and staff members who worked with the patients. When doctors are off-duty and get notifications, they may use an app to check the patient's status from where they are. The app that displays emergency patient wards like ICU and ICCU, etc. They may view the patient's present situation upon selecting the ward. The CCTV concept often applies in this situation. Thus, it is feasible to reduce the death rate and fill in for doctors who are unavailable in an emergency.

The security offered here is that the patient's information can only be obtained by a certain consultant doctor using the patient's secret ID. The restricted number of patients' IDs can be known by the physicians thanks to this security offer for significant individuals.

## CONCLUSION:

This article has covered the several advantages that cloud, and internet of things integration may bring to the e-health industry. We also go through key IoT security flaws in the context of the cloud and highlight current IoT and cloud security solutions that have been specifically designed to safeguard health data. We conclude by suggesting additional security and functionality for bedside cardiac monitors.

## REFERENCES

[1] Imen ben ida., Jemai.,Loukil,"A survey on IoT and cloud in e-health".Networks,2013.

[2] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics. IEEE, 2011.

[3] Bazzani, M., Conzon, D., Scalera, A., Spirito, M. A., & Trainito, C. I." Enabling the IoT Paradigm in E-health Solutions through the VIRTUS Middleware. In Trust, Security and Privacy in Computing and Communications "(TrustCom), IEEE 11th International Conference on (pp. 1954-1959). 2012.

[4] Felipe Fernandez; George C. Pallis "Opportunities and challenges of the Internet of Things for healthcare", Wireless Mobile Communication and Healthcare (Mobihealth), EAI 4th International Conference , 2014.