International Journal of Advance and Innovative Research
Volume 12, Issue 2 (XVII): April - June 2025
ISSN 2394 - 7780

SECURING IOT DEVICES IN HEALTHCARE

[1]Pranav Patel and [2]Wilson Rao
[1]Student and [2]Assistant Professor, MSc. Big Data Analytics Department, Jai Hind College, Mumbai

ABSTRACT
IoMT (Internet of Medical Things) or HIoT (Healthcare IoT) has transformed patient monitoring, improving treatments and streamlining processes, but not without its fair share of risks. By means of a literature survey, this paper aims to examine current research on securing IoMT devices, observing the challenges involved, identifying critical security threats such as the Eavesdropping attacks with categorization of these threats, exploring potential security solutions and various other concepts. Finally, the paper explores future trends such as blockchain, machine learning and artificial intelligence, along with their potential application in healthcare data security.

Keywords—*Healthcare, IoMT, IoT, HIoT, cybersecurity, cryptography, security, vulnerabilities, cyberattacks, encryption, cloud.*

INTRODUCTION
IoT devices are ones that have hardware such as sensors, underlying software and other technologies integrated into them, enabling them to collect data, connect to the internet and share data. They are composed of numerous parts including sensors, actuators, microcontrollers /microprocessors and many more.

Hence, these IoT devices are interconnected physical devices that can collect, exchange, and analyse data.

Healthcare systems have been increasingly employing IoT devices to enhance patient care. These Healthcare Internet of Things (HIoT) systems facilitate remote patient health, monitoring, streamline operations and allow for the control of various medical devices. Data is collected from an individual and their activities. Data is gathered using a variety of body sensors including heart rate body temperature oxygen saturation level (SPo2) and more [5], from an individual and their activities.

Healthcare professionals can use this information to track vital signs, remotely monitor patients and administer timely medical interventions.

With the integration of such IoT devices, there has been an increasing concern for their security. Increased application leads to increase in the attack surface and as these are interconnected, a single piece of vulnerability may expose the entire network, and hence, the confidentiality of the Protected Health & Personally Identifiable Information (PHI & PII) along with the exposed digital infrastructure.

In order to tackle these issues, healthcare institutions need to implement security strategies that include device authentication, access management, network protection, and data encryption to safeguard patient privacy and the security of their information. It is crucial to utilize efficient strategies and tactics to resolve these challenges. In this context, innovative technologies such as blockchain, artificial intelligence (AI), deep learning, and machine learning can play a valuable role in developing new security and protection approaches.

As a result, integrating these IoT devices into healthcare systems presents both significant security challenges and numerous advantages for patient care. The current applications with their security problems and solutions possible, within the healthcare domain are explored further.

HIoT DEVICES
There are a plethora of IoT enabled technologies that are being employed in healthcare. Some of these devices are external in nature, some are implantable and operate within the patient's body, while others can be stationary devices or find applicability as hospital operation tools as well [7].

Some of the external IoT enabled technologies and devices that are being employed in healthcare are as follows:

1. **Wearable health monitors/Fitness trackers/ Smartwatches:** With the development of smart watches, wearable health monitors like Fitbit have provided continuous monitoring of vital statistics. These provide out-of-clinic patient monitoring, which could prove fruitful for any ongoing health conditions, provide care post any surgical operations, as well as for personal health tracking.
2. **Wearable ECG monitors:** They are applied as patches or straps for specialized cardiac monitoring. QardioCore, KardiaMobile and AliveCor are a few examples.

ISSN 2394 - 7780

3. Pulse oximeters: Used to measure oxygen levels in the blood and provide personal and an out-of-clinic experience and they include Masimo Rad-5v and Health Air.

Development of implantable IoT enabled technologies in healthcare has resulted in many devices such as:

4. **Neurostimulators:** These are used to treat conditions like epilepsy and chronic pain by applying electric stimulation to nerves in particular brain regions. Devices include the Vercise DBS System from Boston Scientific and Medtronics InterStim therapy.
5. **Continuous glucose monitors:** These devices are used in homes to track blood glucose levels without requiring a needle prick to draw blood samples. Abbotts Freestyle Libre is one such device.
6. **Cochlear Implants:** Typically fitted in a medical environment, these implants are surgically placed in the inner ear and can greatly benefit individuals with severe hearing impairment. Innovations like the Nucleus 7 and SYNCHRONY 2 cochlear implants have been developed by companies such as Cochlear and MED-EL, respectively.
7. **Intraocular Pressure sensors:** Sensors implanted in the eye are used to treat glaucoma and continuously measure intraocular pressure. Sensimeds Triggerfish is one of the devices that provide both clinical and home-based monitoring capabilities.

There are also several stationary devices apart from the ones mentioned above, that are regularly used in healthcare such as:

8. **Smart beds:** Beds that can adjust for the patient's need through continuous monitoring such Stryker's ProCuity Bed or the Hill Rom Centrella Smart + Bed.
9. **EKG Machines:** IoT-enabled are now employed and provide real time data to the healthcare practictioners for faster recognition of cardiac issues.

IoT technologies are also leveraged in the development of healthcare administration tools such as:

10. **Asset tracking solutions:** Real-Time Location Systems (RTLS) like Stanley Healthcare's AeroScout or CenTrak's offerings, are utilized to monitor the location of important assets such as medical devices or staff in real time, ensuring their optimal utilization.
11. **Environmental monitoring:** Tools such as the Elpro Ecolog-Net system monitor factors like temperature, humidity, and air quality across different areas of hospitals, including operating rooms and storage sites for delicate materials. This enhances patient health and ensures compliance with safety standards.

There are also several cutting edge R&D focused IoT tools being developed such as the Organ on a chip, genetic analyzers and even surgery systems with robot assistance, to name a few.

The summary of application of IoT devices in healthcare is provided in Fig.1.

Aside from the the development of the above mentioned tools and devices, IoT in healthcare is also being used to provide holistic solutions to patient needs and care as [1]:

12. **IoT based ambulances:** An IoT equipped ambulance allows a medical team to remotely recommend the appropriate course of action for the patient. Red Ninja was the first business to create a LiFE (Life First Emergency Traffic Control) algorithm, which modifies traffic light patterns or their durations, for emergency service providers and ambulances
13. **Nexleaf analytics:** This application is greatly useful for immunizations and vaccines in underdeveloped nations. This application conducts monitoring of life-saving vaccine's temperatures within the refrigerator. These vaccines are distributed to clinics and healthcare systems in isolated or rural locations.
14. **Quio:** In the context of COVID-19, this home-based service that is connected via the Internet of Things, shows promise. For instance, IBM and Pfizer collaborated on the IoT-enabled Parkinson House project. By tracking the efficacy of medications and making real-time adjustments if necessary, this improves the doctor-patient connection.
15. **Ambient Assisted Living:** By focusing on senior citizens, it alludes to sophisticated systems of support for a better, safer, and healthier existence in the desired living environment. This method combines wearable and mobile technology with which caregivers can be alerted of hazardous situations to the older people in a house or ambient living facility centres.

ISSN 2394 - 7780

ARCHITECTURE OF IoT DEVICES

Before we discuss the vulnerabilities and security of HIoT systems, it is imperative to develop an understanding of its architecture and its workflow. The architecture of HIoT systems is described as a 4 layer architecture [9] composed of:

1. **Perception Layer:** It contains the physical hardware and it collects data from the environment, which is then sent to the network layer. Simply put, it is the layer data collection layer.
2. **Network Layer:** It connects all the IoT devices in the desired system and allows them to transfer data among themselves. The data is also sent to the base station via technologies such as ZigBee, Wifi, Bluetooth and others.
3. **Middleware Layer:** This layer stores all the procured data from the previous layers, into a database. It includes the services that are used by the application user and allows IoT programmers to work with non-homogenous technologies and to move away from focusing on a specific platform or implementation.
4. **Application / Business Layer*:*** By creating graphs, business models, flowcharts, and other outcomes, this layer—with which the user interacts—is in charge of overseeing all operations and healthcare services. This layer fulfills patient wishes by offering high quality healthcare services.

The major phases in the workflow of an HIoT systems are as follows [9]:

1. **Data generation:** This phase involves the first layer and collects required patient information by various sensors and hardware. It can even include data entry, directly from the healthcare professionals or the patient. The data generated is moved via the second layer.
2. **Data processing:** It involves analysis of the procured data via predetermined algorithms, machine learning methods or other techniques, conducted in the middleware layer.
3. **Data consumption:** The analysed data is finally consumed by the healthcare professionals or personnel for required decision making and can even be used by other systems to trigger actuators to perform some physical application/operation. This phase is performed by the application or business layer.

Fig. 2 illustrates various layers in the HIoT system architecture and the corresponding phases.

NOTABLE CYBER ATTACKS ON IoT DEVICES

IoT devices have their fair share of vulnerabilities that have been exploited in the past, leading to exposure of confidential data, destruction of infrastructure and much more damage [8].

Some notable attacks on IoT systems and devices are:

1. **Mirai Botnet:** The worst DDoS attack was carried out against internet performance management services provider Dyn, in 2016. The attack was performed using the Mirai Botnet, an IoT botnet. The malware-infected computers started looking for susceptible IoT devices on the internet and infected them by entering in with their default identities and passwords.
2. **Verkada hack:** Verkada, a cloud-based video surveillance platform, was hacked in March 2021. The attackers gained access to sensitive information belonging to Verkada software clients and live feeds of over 150,000 cameras mounted in jails, schools, hospitals, and businesses by using valid admin account credentials they could locate online.
3. **Cold in Finland:** Two buildings in the Finnish city of Lappeenranta had their heating switched off by cybercriminals in November 2016. Another DDoS attack then prevented the heating controllers from ever turning on, forcing them to repeatedly reset the system. This attack was severe since Finland has very cold temperatures at that time of year.
4. **Jeep Hack:** In July 2015, the Jeep SUV's security was inspected by a group of experts. By exploiting a vulnerability in a firmware upgrade, they were able to take over the car. After that, they could manage the car's speed and even take it off the road.
5. **Stuxnet:** Stuxnet is probably the most famous IoT attack. Its target was a uranium enrichment plant in Natanz, Iran. During the hack, the Siemens Step7 software running on Windows was compromised, allowing the malware to access the industrial program logic controllers. This allowed the virus developers to gain access to vital industrial data and gain control of several pieces of equipment at the industrial sites. This malware is thought to have damaged 984 uranium-enrichment centrifuges. According to estimates, this resulted in a 30% drop in enrichment efficiency.

ISSN 2394 - 7780

Among the many IoT enabled devices that find themselves being employed in the healthcare domain, some of the vulnerable IoT devices found among them are:

1. **Insulin and Infusion pumps:** These can administer blood, saline and other fluids, remotely, which decreases costs and assures quality of patient care. But these devices can be disrupted by exploiting the connectivity capabilities present in them.
2. **Smart pens:** There is some amount of patient data stored in smart pens that are an attractive target to cybercriminals. In addition to the data stored on the pen, it can also be used as an entry point to medical record databases and more. A cybersecurity researcher had exploited this very vulnerability in 2017.
3. **Implantable cardiac technology:** Devices like pacemakers and their programming devices, have potential to kill, as researchers have discovered that a simple DOS attack on these devices can prove fatal.
4. **Thermometers and temperature sensors:** There was a case wherein a casino was hacked via their fish tank's smart thermometer. Such a case only serves to show that security is a critical aspect in IoT enabled technology in healthcare and vulnerabilities have to be assessed carefully to avoid such exploitations.

SECURITY THREATS IN HIoT

There are several reasons for cyber attacks in HIoT devices such as monetary value of the data and its potential for malicious activities, regulatory compliance restrictions that may lead to difficulties, and limited resources for security mechanisms, among others. The reasons are illustrated in Fig. 3 [18].

In a recent study, HP examined a variety of widely used Internet of Things devices, including thermostats, door locks, webcams, and home alarms. The company discovered that a startling 70% of the devices used unencrypted network services. Furthermore, most did not encrypt data while it was in transit [4].

IoT device vulnerabilities are frequently the result of ignorance or the connection of technologies that were not initially thought to pose a risk as a separate entity. Since the name "IoT" refers to a broad category of devices, and since HIoT gadgets may have socioeconomic ramifications, the scope of these risks and exploits is enormous.

References [5], [6], [13], [17] discuss the various security issues and concerns faced in HIoT which are:

1. **Identity Management and Authentication:** IdM and authentication use a combination of technologies and procedures to secure and control access to data and resources while safeguarding the "things" profile. IdM gives items a unique identification, and authentication entails confirming the two communicating parties' identities.
2. **Data Integrity:** Information must be shielded from outside alteration. Life-critical patients suffer significant harm as a result of the lack of integrity. Data loss can also happen in an unfavorable communication environment.
3. **Authorization:** Preventing unauthorized user participation is crucial since an application may have an arbitrary number of users. Once recognized, authorization enables us to ascertain if the individual or item is permitted to possess the resources. Usually, access controls are used to implement it. Authorization and access control are required to establish a secure connection between several devices and services.
4. **Data aggregation:** Wireless sensor networks frequently experience node failures, hence a safe data accumulation technique is required to guarantee that accurate data is gathered from sensor nodes across the network.
5. **Data confidentiality:** In many situations, maintaining data confidentiality is the primary limitation.
6. **User Privacy and anonymity:** If any intruder overhears the vital information of a patient, it can be used with malicious intent, which can cause several psychological and emotional distress to the patient, further worsening their condition.
7. **Data Freshness:** Attackers may capture data in transit and may transmit it repeatedly to confuse the coordinating node. Hence, the freshness of the data may be lost. Also, data freshness is imperative since healthcare personnel need real time updates of the patients, and lack of data freshness can hamper their decision making ability.
8. **Secure localization:** Since the sensors and devices gather location data, this information must also be shielded from misuse.

ISSN 2394 - 7780

Some common security attacks in the healthcare systems are presented such as phishing attacks to trick individuals to provide sensitive information, insider threats by misuse of access privilege, jamming attack to block communication, desynchronization attack by introduction of loops to waste energy, and sybil attacks through embodiment of multiple personas within the network [18].

Fig. 4 represents the common types of cyber security attacks.

Since we have explored the various issues and attacks faced by IoT systems, we need to understand the limitations of these devices, that hamper their security functionalities. The two major limitations are presented as [13]:

16. **Battery life:** Since some IoT devices are placed in locations without charging, they possess a very limited amount of energy, and hence, strict security settings may cause the devices to use up all of their resources. To lessen this problem, there are three potential strategies. The first of them is to employ minimum security requirements, which is not advised, particularly when handling sensitive data. Increasing the battery's capacity is the second strategy. Nonetheless, the majority of IoT devices are made to be compact and light. No additional space is available for a larger battery. The last strategy is to use natural resources (such as light, heat, vibration, and wind) to generate energy, however this would necessitate a hardware upgrade and greatly raise the cost.
17. **Lightweight computation:** The computing as well as storage requirements for any advanced cryptographic techniques are hindered due to limited memory space.

IoT attacks can broadly classified based on the layer affected as:

1. **Physical attack:** It is usually performed given the attacker is in close proximity to the device.
2. **Network attack:** Involves manipulation of the network, leading to damage.
3. **Software attack:** Occurs due to exploitation of vulnerabilities in the IoT application.
4. **Encryption attack:** Breaking the system encryption.

The attacks on HIoT devices into can also be segregated into 5 major categories depending upon the type of the attack taking place:

1. **Selective forwarding:** Herein, packets are forwarded selectively by malicious nodes to disrupt the routing path.
2. **Sinkhole attack:** It involves an infected node attracting nodes in proximity and causes them to route the traffic through it. When coupled with selective forwarding, this attack becomes very powerful, and all the information is sent to the attacker who can profile the patient through their information.
3. **Jamming:** This is a classified machine-to-machine attack that uses a noise signal to occupy the wireless band, obstructing communication between Internet of Things devices and producing interference.
4. **Flooding:** The goal of this attack is to disrupt the transmission by repeatedly establishing connection requests and using the target resources.
5. **Phishing:** A technique used to steal data and personal information.

Since eight out of ten organizations reported experiencing a cyberattack on their IOT devices in 2019, IOT security becomes increasingly important as its adoption grows. Ninety percent of those organizations were impacted by the hack, which included compromising customer data or end-user safety as well as operational outages [11].

Hackers "killed" (simulated) patients at the 2018 RSA Conference USA without the doctors even realizing the operating room had been compromised. The simulation illustrated how dangerous it is for IOT device vulnerabilities to put a patient's life at risk without the present medical staff's knowledge.

Over the past five years, cyberattacks have generally increased by 125% in healthcare ecosystems. One healthcare organization owned 12,000 of the more than 68,000 medical systems that two security researchers found to be online in late 2015. The figures show the degree of threat posed by IOT devices and the hazards involved, should they be penetrated by malicious actors that could interfere with system functionality and steal personal data.

ISSN 2394 - 7780

A number of research investigations to expose security issues displayed, that such devices were connected to systems running on Windows XP, which is known to have its fair share of vulnerabilities. A search engine called Shodan which can find IoT devices connected to the internet, was used to find these devices.

Two researchers used Shodan to locate MRI scanners, pacemakers, nuclear medical systems, infusion systems, anaesthetic equipment, cardiology devices, and other gadgets. Because even script kiddies can exploit these flaws, the threat is serious. Researchers looked into these gadgets' exposure, and the CIA triad was used to gauge their influence.

To address the growing concern of cybersecurity in medical devices, the Food and Drug Administration (FDA) has created cybersecurity standards for three kinds of medical devices before the devices are put on the market.

1. MEDICAL DEVICE CLASSES

Medical Device Class	Attributes	Example Devices
I	Common devices with low risk and low complexity	Lancet, Dental Floss
II	More complex devices with a greater risk to the patient, partially implanted	Syringe, Insulin pumps, BGM
III	Fully implanted devices with greater risk, such as Replacement Heart Valves	Artificial Pancreas, CGM

Hence, there is a need for experts and researchers to prioritise their focus in securing the Class II and III medical devices

LITERATURE REVIEW

IoT devices should include network segmentation and monitoring in order to detect any unusual traffic [4].

One major security concern is the use of insecure passwords and Wi-Fi and routers with their default security configurations and passwords. As per OWASP, the most common vulnerability in IoT devices is weak passwords. Users frequently forget to change the default passwords or don't follow best practices for creating strong, secure passwords. The security implications of the HIoT are just as important, notwithstanding its potential to promote socioeconomic progress and health-related wellness.

Table II illustrates the numerous dangers for each tier of the standard HIoT architecture.

Reference [14] discusses the classification of IoT attacks and the different security issues across the layers. It explores the security and privacy requirements of HIoT devices and underlines 4 requirements involving data integrity, its usability, data auditing and privacy involving patient information.

2. SECURITY THREATS IN IOT ARCHITECTURE [3]

Layer	Description	Threats
Cloud	Data center cloud layer/cloud network host applications that are critical providing IoT services.	Data interruption, DDoS, Buffer overflow, Impersonation, Remote code execution
Core	The function of this layer is to carry and exchange data and network information between multiple subnetworks.	Data interruption, Man-in-the-middle (MITM) attacks, Impersonation/Spoofing, Modification of data at rest and in transit, Relay attack, Confidentiality attack, Jamming/Congestion, Data exchange issues: data privacy, access control, and disclosure of information

ISSN 2394 - 7780

Edge	Endpoint devices with both wired and wireless connectivity. This scalable layer supports Zigbee, IEEE 802.11, 3G and 4G.	Connection flooding, Data interruption, DoS, Eavesdropping, Impersonation, Jamming attack, Modification of data at rest and in transit, Misconfiguration, Network protocol vulnerability and exploit, Packet manipulation, Physical attack/tampering, Rogue access points
Things	Embedded systems and sensors. Small devices with varying OS, CPU types, memory, network capability.	Authenticity, Device end-point attack, Counterfeiting attacks, Eavesdropping, Hardware interruption/theft/modification, Jamming attack, Resource exhaustion, Privacy, Spyware, Repudiation, Device specific vulnerabilities, ie. OS vulnerabilities, malware, weak authentication, etc

THE EXISTING SOLUTIONS AS DISCUSSED FURTHER AS

1. **Data encryption:** Three degrees of implementation are possible. Initially, as link encryption for data transmission between links. The second is node encryption, which prevents the network node from receiving messages in plaintext. Third, end-to-end encryption, which means that until the message reaches its destination, it cannot be decrypted.
2. **Access control:** One can employ symmetric, asymmetric or attribute-based key encryption.
3. **Trusted third party auditing:** The Trusted Third Party (TTP) provides unbiased audits results to guarantee that cloud service providers are held responsible and to protect the legitimate benefits of cloud users.
4. **Data search:** Enabling an encrypted cloud data search service is essential. The two primary methods for searchable encryption are public-key encryption with keyword search (PEKS) and searchable symmetric encryption (SSE)..
5. **Data anonymization:** Patient sensitive data can be divided into three categories: explicit identifiers, quasi-identifiers, and privacy characteristics. Explicit identifiers that can be used to uniquely identify a patient include an ID number, name, and mobile phone number. A combination of quasi-identifiers, such as age, address, and birth details, can also be used to uniquely identify a patient. The term "privacy attributes" refers to sensitive patient characteristics, such as illness and income. The distribution characteristics of the original data must be taken into consideration while handling the individual attributes of the new dataset during the data publishing process in order to protect patient privacy.

Additionally covered are the use of lightweight cryptographic methods for effective database query processing over encrypted data and encrypted query processing for cloud storage. Additionally, lightweight encryption strategies for smart homes based on stateful identity-based encryption and a method to lower latency by dividing query results into discrete data sets have been explored.

Reference [5] discusses the security issues and remediation measures across the layers, as:

18. Lightweight cryptographic techniques are employed in the perception layer to allow for security.
19. Counterfeit and Man in Middle attacks are belong to the threats that affect the IoT network layer. Both of these techniques have the ability to send false information while simultaneously capturing information
20. At the IoT application layer, data exchange can lead to information disclosure and security issues with privacy and access control.

A secure HIoT system is proposed, which consists of 3 communication channels:

21. Sensor nodes (the edge sensors) to the internal processing unit (IPU),
22. Internal processing unit (IPU) to gateway (router)
23. Gateway to the cloud.

ISSN 2394 - 7780

The suggested approach uses three distinct security protocols for the three types of communications channels: SHA-3, AES-256, and HTTP-SSL, respectively. Additionally taken into consideration is the biosensor devices' registration.

The registration process involves using RSA-1024 by the IPU to share the public key to nearby bio-sensors. Using this public key, the sensor encrypts its own symmetric key and shares it back with the IPU, hence they now share the secret key.

Now the ID of the sensor is encrypted using the secret key, which is then decrypted by the IPU and stored as hashed values.

When a sensor sends the data, it sends the ID along with it. This ID is matched against the hashed values and hence, verifies the sensor. A basic implementation environment was also provided for the above solution. This proposed scheme aims to solve the issues of access control, authenticity, confidentiality, and integrity.

Reference [6] proposes a secured architecture of 3 layers, represented in Fig. 5, as:

1. **Device/Sensor Layer:** Wearable sensor and data acquisition units.
2. **Network layer:** Networking and communications
3. **Backend:** Processing and analysis

The security across these layers is discussed as follows:

1. **Device/Sensor Layer:** In this case, local processing is used to prevent unauthorized users from identifying the data's source when it is being transferred over a wireless network. Symmetric key cryptography is proposed.
2. **Network Layer:** In this layer, man-in-the-middle attacks are common. Public key or symmetric key cryptography is required. The software that acts as a bridge between cloud computing services and smart devices is the IoT gateway, which provides security and other services like data or protocol translation as well.
3. **Backend:** Here, data is analysed and users can query the data available on cloud or on other sources. This layer requires strong security in the form of anti-virus, public key cryptosystem, and other protocols.

The paper concludes with a discussion of cryptography and its forms, and the types of cryptography involved in this proposed architecture.

By way of a literature review, authors in [10] explore various concepts in HIoT including the security issues prevalent in them. It explains importance for aversion to DoS attacks at the network layer and the inclusion of lightweight cryptography owing to its efficiency.

The healthcare system attacks can be defined into the following categories:

24. Physical attacks include assaults on the physical hardware
25. Side channel attacks use information to determine the key being used by the target device.
26. To crack the encryption, cryptanalysis attacks are carried out.
27. Software assaults utilize the communication interface of the program itself in search for flaws.
28. Network communications are susceptible to network security attacks due to the broadcast nature of the transmission channel. Most IoT-based frameworks are vulnerable to various security threats, such as covert assaults on availability, authentication, and service integrity.

Reference [12] suggests a cloud based model for future HIoT systems, comprising of:

1. **Wearable sensors:** Wearable sensors are ones that collect all the patient data and the central node will receive this data, which subsequently processes it and may even implement any decision making involving information forwarding to another location.
2. **Short Range communication:** To transfer data from the sensor to the central node. These should be low latency, have robust security features, and should not negatively impact human health.
3. **Long range communication:** Data from the central node is sent to a database considering latency, security and several other characteristics.

ISSN 2394 - 7780

4. **Secure Cloud Storage Architecture and ML:** Using cloud storage to store the vast amount of sensor data generated and machine learning for trend identification, diagnosis assistance and patient specific recommendations.

The authors have also provided several use cases for their proposed system such as:

1. A wearable accelerometer sensor-based knee injury rehabilitation system.
2. To create systems that can help control long-term illnesses like high blood pressure.
3. Tracking alterations in patients suffering from degenerative illnesses like Parkinson's disease.

The security considerations in employing cloud for HIoT systems are resolved via access control policies and data encryption. Several security mechanisms are discussed such as:

29. **SafeProtect:** Focuses on patients creating a policy to only allow limited access to their data and have control over their information. This mechanism only allows validated healthcare providers to access the data via credentials and prevent illegal actions as per access policies that are set.
30. Signal scrambling, which uses "tiny data," a small fraction of the data that is transferred among authorized parties and serves as a scrambling key.
31. A fully homomorphic encryption is assessed and a steganography-based solution to access control is examined. FHE makes it possible to encrypt data using public keys and perform mathematical operations on it without having to decrypt it in the cloud.
32. FHE was also compared against the AES and Attribute-Based Encryption (ABS).

The security discussion concludes with a suggestion for an optimised ABE-to-FHE conversion scheme, which would be extremely valuable to the patient data.

Authors in [16] discuss some of the security issues in HIoT systems across the layers.

33. The physical layer is vulnerable to impersonation and denial of service attacks. Tampering of the nodes, injecting malicious data, modification of the routing path of the devices during the process of forwarding of the data, and packet sniffing are the attacks that the physical layer must prevail through.
34. At the network layer, security for routing attacks, denial of service and data transit attacks have to be employed.
35. Finally, the application layer is exposed to leakage of data, and injection attacks among others.

Solutions to these privacy issues are described, including automated threat detection and response, and Data Provenance, a tool that aids in recovering data from its original location to its whole history chain. Any changes made to the data during its lifespan are recorded. This aids in confirming any modifications made to the data that might result in abuse. To obtain the data provenance associated with a certain patient, a range of data models are available. Strong network security can be achieved by the use of techniques including confidentiality, access control plans, and authentication. The paper concludes with a suggestion that a single solution may not solve the security and safety issues. Patient data safety and cyber security must advance more quickly than policy implementation and regulation. To use the linked devices in the future, the Internet of Things need higher requirements every day..

Reference [17] explored several security solutions to the problems have been explored via a systematic survey, which include the following measures:

1. To enable secure network communication, lightweight authentication techniques use straightforward cryptographic hash functions. The devices' identities are concealed through the use of hash and XOR operations.
2. To ensure safe communication between the IoT client and IoT server, an addressless IoT server is used.
3. To examine problems with patient data collection, researchers have turned to kHealth, an Internet of Things-based healthcare information monitoring system.
4. A cloud-based user authentication system has been used by researchers. To ensure safe conversations, it includes a private session key. In order to verify the resilience against well-known attacks, the authors also conducted a security study of the developed mechanism using a Real-OrRandom model.

The authors have then defined a security benchmark for the IoT architecture. This benchmark includes an evaluated score to determine the strength of the security.

ISSN 2394 - 7780

The security requirements for said benchmark were outlined as follows:

1. Authentication
2. Confidentiality
3. Integrity
4. Self-healing: restoring to working state when a node failure occurs
5. Fault tolerance against failed components, resilience to attacks even when system/service failures take place
6. Data freshness
7. Trust related to access control and identity management
8. Firewall configuration
9. TLS/SSL for encrypted communication, certificates signed by a certification authority, and regular software updates.

The authors then provide their proposed AMI (Ambient Intelligence) Lab architecture with the 3 layers involving a cloud architecture. The security in this framework is provided via a secured channel with authentication from both ends, firewall configuration at gateways, using gateway address to avoid data stealing instead of user identity, presence of a middle node to limit communication, and cloud server security configuration. Security agents are deployed on the cloud and in the nodes to sense any and all intrusions.

The network layer uses 2 servers for securing communication and is being accountable for creating SSL certifications. It also employs TCP for communication, data authentication using SHA-2, use of a VPN server and using Elliptic Curve Diffie Hellman to encrypt the communication handshake.

The authors analyse their proposed framework against the security benchmarks to evaluate how it stands against the requirements.

Reference [18] discuss the structure of a smart healthcare systems comprising of the medical devices, sensors, networking components like Bluetooth, data processing capabililities to obtain insights about health conditions & the health provider which provides remote or in-person treatment.

The authors have further detailed the security schemes as per the levels and their functionalities as:

1. **Data level:** It entails confidentiality of patient data, integrity to ensure quality, efficiency and consistency of the data throughout its cycle, and availability to ensure accessibility of records whenever needed.
2. **Sensor Level:** It entails tamper proof hardware using Physically Unclonable Features, sensor localization, self-healing sensors, over the air programming to update devices with new security policies and patches, and forward and backward compatibility which signify that the messages must not be readable once they leave the network and previously transmitted messages must not be readable by sensors that have just joined the network.
3. **Personal Server Level:** The data is collected and aggregated on the server level hence 2 types of authentication are needed. Device authentication is needed to ensure that data is accepted from authenticated devices. User authentication is needed via biometric authentication or other strategies.
4. **Medical Server Level:** It includes access control, key management, trust management between 2 nodes and resistance to DoS attacks.

Several open issues and challenges in IoMT Based healthcare system, network and protocol challenges are discussed.

Reference [19] provides an overview of the different methods for encryption in IoT in healthcare. They discuss the 2 categories of encryption, symmetric and asymmetric.

36. Asymmetric key encryption employs a pair of keys, such as public and private keys, for encryption and decryption, whereas symmetric key encryption uses a single key.
37. The AES is an extensively used symmetric key encryption which is also a lightweight cryptographic algorithm and provides good security and balance performance in low-power IoT devices.

ISSN 2394 - 7780

38. Because of their simplicity and effectiveness, the lightweight block ciphers known as Speck and Simon are ideal for Internet of Things applications. Secure key management is necessary for symmetric key encryption, though.
39. Asymmetric key encryption has Elliptic Curve Cryptography which has high processing efficiency with strong security and small key sizes, hence it is an excellent choice. Quantum Key Distribution uses quantum mechanics to allow safe exchange.

The authors have then gone on to discuss the lightweight cryptography which involves LEA (Lightweight encryption algorithm) and PRESENT. Key management via Hardware Secure Modules (HSM) which provide a secure environment for managing keys, and secure key exchange protocols such as Diffie Hellman Key Exchange.

Hardware based security solutions include Trusted Execution Environments (TEEs) to process sensitive data, and Secure Elements (SEs) which are tamper resistant hardware components that store sensitive information and perform cryptographic execution.

The authors also provide an outline of several challenges and future directions involving standardisation of security protocols, interoperability between devices from different manufacturers, and the evolving threat landscape.

The authors provide the performance comparison of different encryption algorithms wherein Speck-64 and PRESENT algorithms outshine the others in processing time, minimum computation overhead and resource utilisation.

Among the security evaluations, AES-256 and ECC (256-bit) proved to be highly resistant to brute-force, known-plaintext and side-channel attacks.

The impact of encryption on the patient data transmission efficiency revealed that Speck-64 and PRESENT had higher data transfer rates and low latency.

ECC (256 -bit) which provides robust security, results in lower transfer rates and higher latency.

FUTURE TRENDS

Blockchain

Reference [2] discusses blockchain technology as a solution to the data fragmentation issue. Three aspects contribute to blockchain technology's secure transmission:

40. It features an unchangeable "ledger" that people can access and manage. There are set guidelines that must be followed for each transaction in the ledger.
41. Secondly, blockchain is a distributed system that runs concurrently on several computers, devices, etc.
42. Third, blockchain adheres to agreement standards and data exchange policies through the use of smart contracts. Identity control and access privileges to different blockchain-stored electronic medical reports (EMRs) are established by the smart contract. It suggests that doctors are limited to using the EMRs to which they have been given access.

Additionally, the authors investigate the creation of a blockchain-based application called Healthcare Data Gateway (HDG). It allows patients to share their information and ensures that privacy policies are not violated. The architecture of the same is displayed in Fig. 6.

Reference [18] also discusses blockchain as a part of the future trend to deliver robust and broad security with privacy protection. However, blockchain technologies demand significant resources, hence it may not be feasible in IoMT systems, but can be used to store data on medical servers. An example of this is MedRec, which has pioneered research into using blockchain to manage access to medical data

MACHINE LEARNING

Machine learning models for predicting and prognostics, enhancing production process efficiency with low maintenance costs, and minimizing product quality deterioration are covered in Reference [4]. Their method of analyzing sensor data would be very beneficial for e-health and wellness in the context of H-IoT.

A machine learning classifier with 4 experiments was further discussed to assess the most significant feature in classifying an IoT connection as normal or anomalous. The connection record consisted of 100 bytes.

ISSN 2394 - 7780

The four experiments conducted were:

1. **Correlation-Based Feature (CSF) Subset Evaluation:** The predictive power of each characteristic and the level of duplication among them are taken into account when evaluating the value of a subset of attributes. Consequently, the top ten predicted characteristics were determined, including protocol type, connection time, and others.
2. **Gain Ratio Attribute Evaluation:** Selecting the most predictive feature based on an "average merit". This resulted in features such as logged_in, srv_error_rate and few others being introduced in the top 10 which were previously unworthy.
3. **Information Gain Attribute Evaluation:** This experiment measures the information gain in relation to the class, in order to assess the value of an attribute.
4. **K-means clustering analysis:** This experiment aimed to cluster connections into attack or normal, but the results generated a pretty high error rate. Hence, no clear distinctions between the classes could be determined without employing other techniques.

The authors draw the conclusion that while the dataset seems to have an even class distribution, which is advantageous for machine learning, these circumstances are unlikely to arise in a real-world setting because the attack data would be greatly outnumbered by the normal data. As a result, the machine learning technique that has been explained would not yield positive outcomes when applied to a bigger dataset. Because Deep Learning can learn and make much more concise conclusions, the article recommends it as a suitable technique for granular analysis.

ARTIFICIAL INTELLIGENCE

Reference [18] also discusses AI as a future trend in IoMT systems.

The authors discuss the challenges of generative AI in healthcare systems. Several security issues arise as these systems can be manipulated to generate false data or misleading predictions, if not secured properly. It also increases the surface area for potential breaches. Other issues are data bias and the reliability of AI generated outcomes

Ensuring the privacy and security of sensitive patient data, navigating the ethical and legal complexities of AI decisions, achieving seamless integration and interoperability with existing healthcare IT infrastructures, and adapting the healthcare workforce to leverage AI technologies effectively, are some of the challenges involved.

As medical service providers are exploring the use deep learning techniques for diagnosis, its imployement for systems security and privacy is also an example of research to consider. Herein, PHI is searched at different layers of IoMT systems to detect centralised attacks through deep learning networks.

Objectives of Study

The main objective in this study was to identify the applications of IoT devices in healthcare systems, and analyse the various security issues that arise in their implementation. The security challenges identified herein were also resolved via different forms of encryption, access control, cloud implementation and many others. Several innovative and future trends were put forth such as blockchain technology, artificial intelligence, and their involvement to resolve potential vulnerabilities in security systems.

This paper aimed to provide the reader with a holistic view of the HIoT systems particularly conforming to its security aspects, exploitation and solutions, and the hope for future advancements.

Scope and Limitations

HIoT systems will continue to see more and more growth and popularity owing to their applicability in various medical situations. However, several research directions must be exploited in order to safeguard such systems. Several innovative solutions can be applicable in this context, such as:

1. **AI:** Inclusion of AI models to detect intrusions and attacks. These models are even utilised currently for various medical diagnosis and identification of medical conditions, progression and other situations. However, solutions and data offered by these models must also be verified for their accuracy, since these models are known to make errors.
2. **Blockchain:** This technology shows promise in the terms of the security offered by it. However, further research has to be conducted to understand inclusion in existing IoT systems, keeping in mind the energy efficiency of these systems and the scarcity of resources available to them.

ISSN 2394 - 7780

3. **Deep learning:** For intrusion detection and prevention of common attacks such as man in the middle attack or internal security threats.

The major issues that limit the security mechanisms applied in IoT systems are resource scarcity or limited computation. Hence, research efforts must specifically keep these in mind while developing novel techniques for security or even for healthcare applications, in general.

CONCLUSION

This study highlighted the various applications of IoT systems in healthcare. It identified the reasons for popularity of these systems as targets for cyber attacks and the various attacks that commonly occur. The major security considerations for such systems and exploration of possible encryption techniques, cloud architecture, blockchain and AI inclusion has been considered. The realm of HIoT is a vast field that has to be carefully trodden while developing novel applications and solutions for the protection of the patients and solutions for their care.

FIGURES

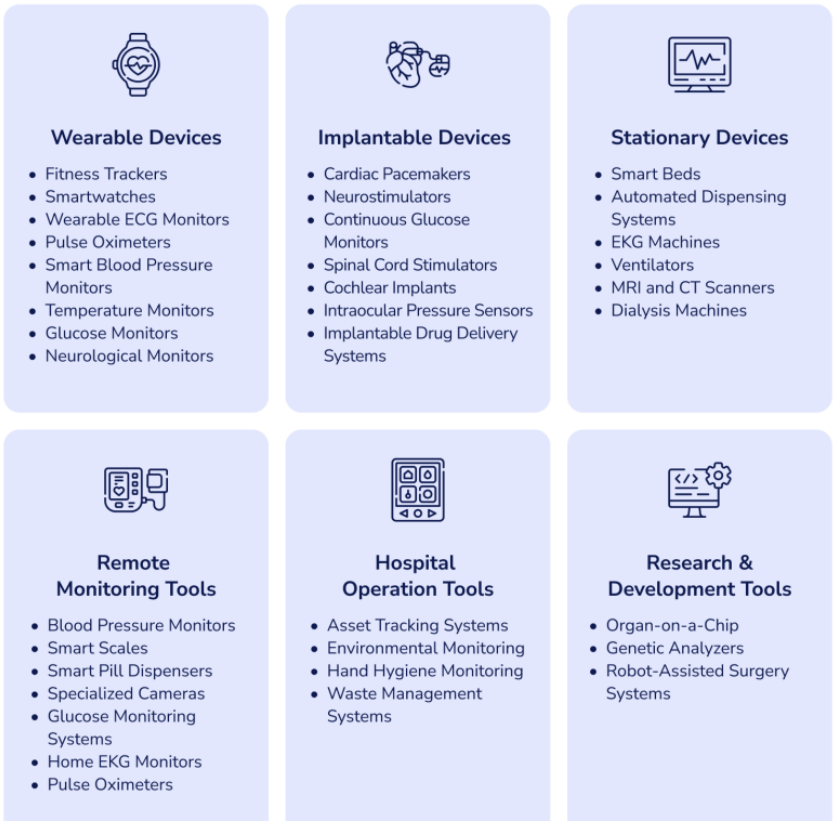

Fig . 1. IoT Devices in Healthcare Taxonomy [7]

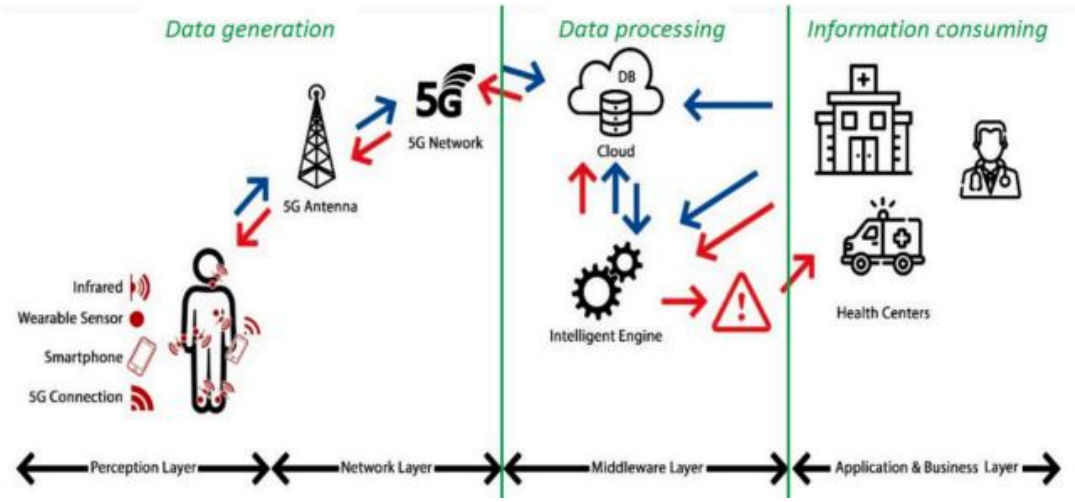

Fig. 2. Architecture of HIoT Systems [9]

ISSN 2394 - 7780

Fig.3. Reasons for cyber attacks on IoT systems. [18]

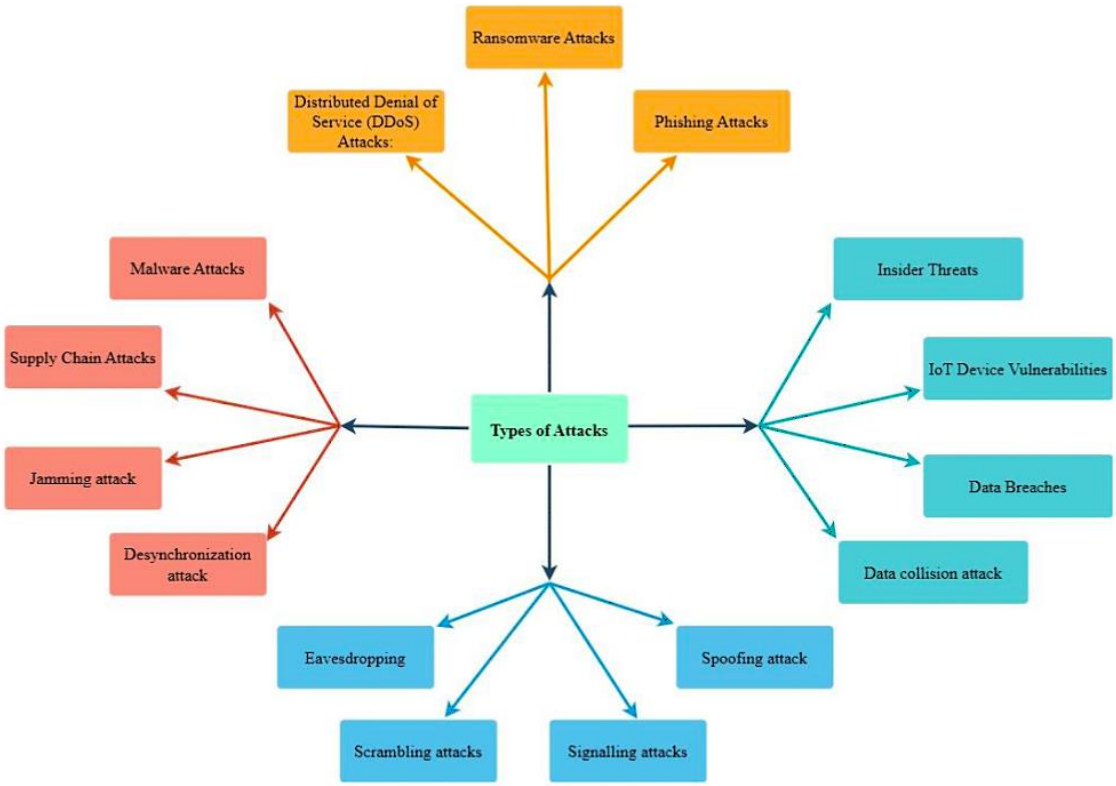

Fig. 5. Types of cyber security attacks on IoT devices. [18]

ISSN 2394 - 7780

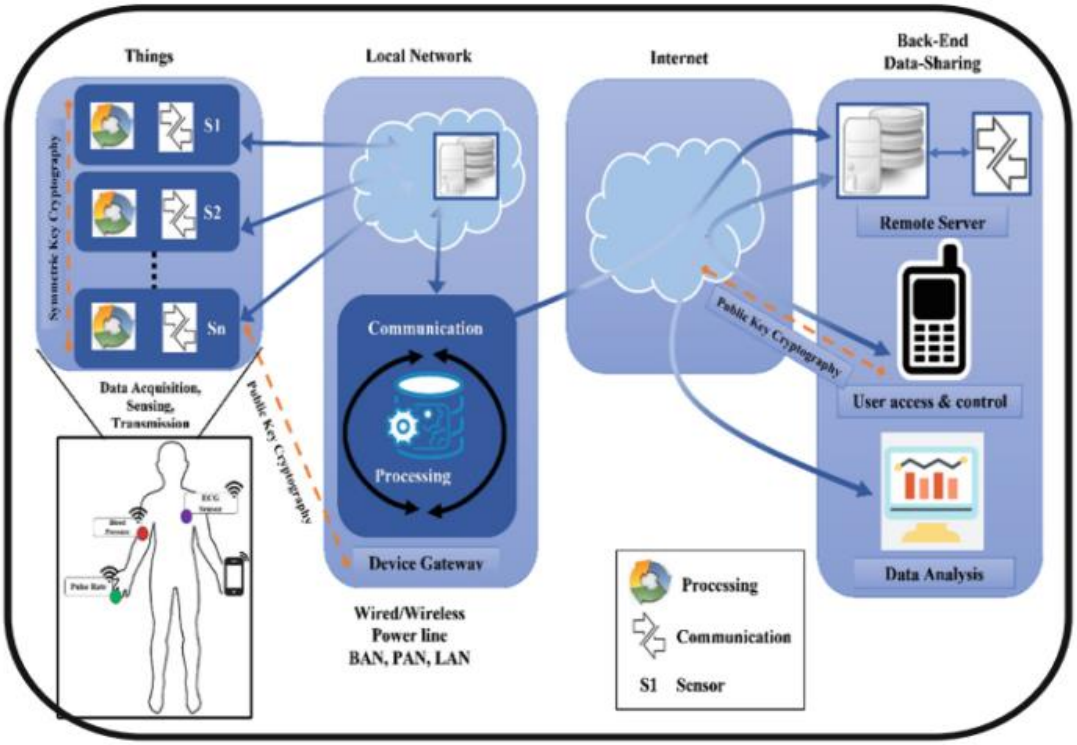

Fig. 5. A secured architecture for HIoT system [6]

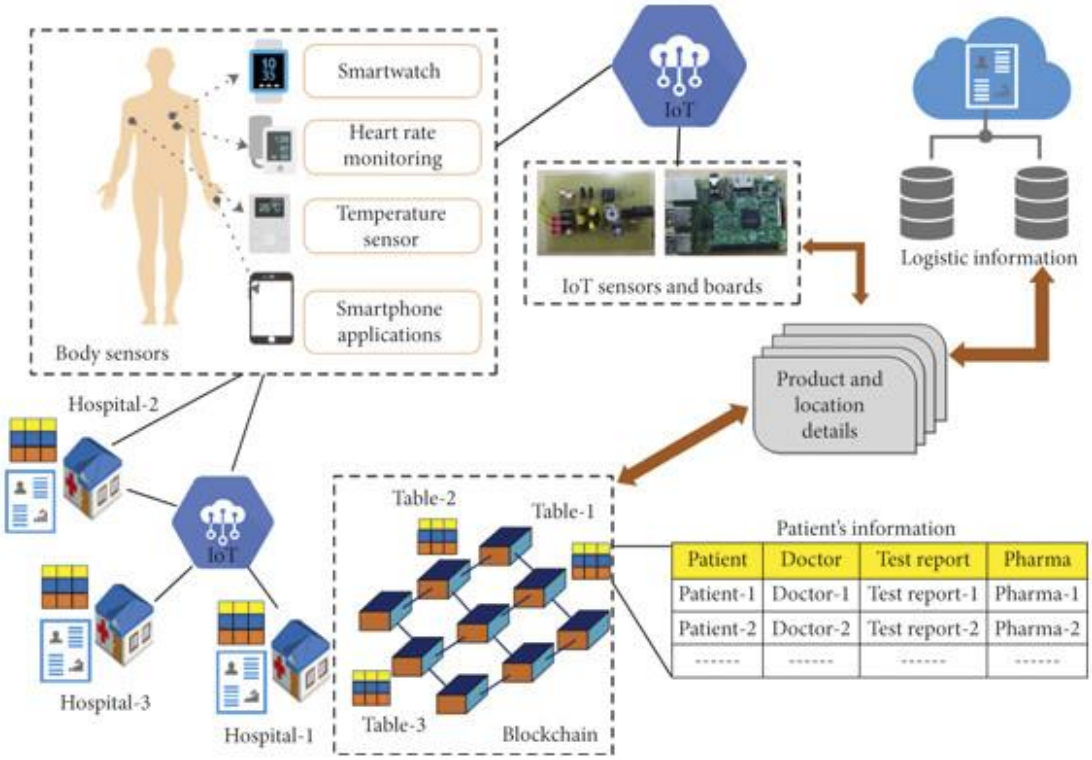

Fig. 6. An architecture of HIoT system with the inclusion of blockchain [2]

ACKNOWLEDGMENTS
I would like to express my deepest gratitude to all those who have supported me throughout the course of this research.

First and foremost, I would like to thank my mentors, Prof. Wilson Rao, for their invaluable guidance, expertise, and encouragement. Their constant support and insightful feedback were crucial to the completion of this study.

ISSN 2394 - 7780

I would like to acknowledge the contributions of my peers for their support, insights and constructive feedback. Your assistance have been proven to be a great asset.

Finally, I am forever indebted to my family and friends for their unwavering love, patience, and moral support throughout this journey. Their encouragement and belief in me have been a source of strength, especially during challenging times.

REFERENCES

- Al-kahtani, Mohammad S., Faheem Khan, and Whangbo Taekeun. 2022. "Application of Internet of Things and Sensors in Healthcare" Sensors 22, no. 15: 5738. doi: 10.3390/s22155738
- Pradhan, Bikash, Bhattacharyya, Saugat, Pal, Kunal, IoT-Based Applications in Healthcare Devices, Journal of Healthcare Engineering, 2021, 6632599, 18 pages, 2021. doi.org/10.1155/2021/6632599
- Kumar, Mohit, Ashwani Kumar, Sahil Verma, Pronaya Bhattacharya, Deepak Ghimire, Seong-heum Kim, and A. S. M. Sanwar Hosen. 2023. "Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues" Electronics 12, no. 9: 2050. doi.org/10.3390/electronics12092050
- Á. MacDermott, P. Kendrick, I. Idowu, M. Ashall and Q. Shi, "Securing Things in the Healthcare Internet of Things," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766383.
- Chattopadhyay, A.K., Nag, A., Ghosh, D., Chanda, K. (2019). A Secure Framework for IoT-Based Healthcare System. In: Chakraborty, M., Chakrabarti, S., Balas, V., Mandal, J. (eds) Proceedings of International Ethical Hacking Conference 2018. Advances in Intelligent Systems and Computing, vol 811. Springer, Singapore. doi.org/10.1007/978-981-13-1544-2_31
- Vithya Vijayalakshmi, A., Arockiam, L. (2020). A Secured Architecture for IoT Healthcare System. In: Pandian, A.P., Senjyu, T., Islam, S.M.S., Wang, H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer, Cham. doi.org/10.1007/978-3-030-24643-3_106
- Yury Shamrei, 2024's Top IoT Devices Transforming the Healthcare Landscape, Sumatosoft, https://sumatosoft.com/blog/top-iot-devices-transforming-the-healthcare-landscape
- Alex Husar, IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities. https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities
- Mostafa Haghi Kashani, Mona Madanipour, Mohammad Nikravan, Parvaneh Asghari, Ebrahim Mahdipour, A systematic review of IoT in healthcare: Applications, techniques, and trends, Journal of Network and Computer Applications, Volume 192, 2021, 103164, ISSN 1084-8045, doi.org/10.1016/j.jnca.2021.103164.
- Marques, Gonçalo, Rui Pitarma, Nuno M. Garcia, and Nuno Pombo. 2019. "Internet of Things Architectures, Technologies, Applications, Challenges, and Future Directions for Enhanced Living Environments and Healthcare Systems: A Review" Electronics 8, no. 10: 1081. doi.org/10.3390/electronics8101081
- Abdi, Isse, "IOT Devices in Healthcare: Vulnerabilities, Threats and Mitigations" (2023). Culminating Projects in Information Assurance. 139. repository.stcloudstate.edu/msia_etds/1394
- S. B. Baker, W. Xiang and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," in IEEE Access, vol. 5, pp. 26521-26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
- Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.
- Sun, Wencheng, Cai, Zhiping, Li, Yangyang, Liu, Fang, Fang, Shengqun, Wang, Guoyan, Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks, 2018, 5978636, 9 pages, 2018. doi.org/10.1155/2018/5978636

ISSN 2394 - 7780

- Akshay Parihar, Jigna B. Prajapati, Bhupendra G. Prajapati, Binti Trambadiya, Arti Thakkar, Pinalkumar Engineer, Role of IOT in healthcare: Applications, security & privacy concerns, Intelligent Pharmacy,2024,ISSN2949-866X, doi.org/10.1016/j.ipha.2024.01.003.
- Ibrahim Sadek, Josué Codjo, Shafiq Ul Rehman, Bessam Abdulrazak, Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment, Computer Methods and Programs in Biomedicine Update, Volume 2, 2022, 100071, ISSN 2666-9900, doi.org/10.1016/j.cmpbup.2022.100071.
- Bala, Indu, Irfan Pindoo, Maad M. Mijwil, Mostafa Abotaleb, and Wang Yundong. "Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence". Jordan Medical Journal 58, no. 3 (July 15, 2024). Accessed October 30, 2024. jjournals.ju.edu.jo/index.php/JMJ/article/view/2527.
- Vishwasrao Salunkhe, Abhishek Tangudu, Chandrasekhara Mokkapati, Prof.(Dr.) Punit Goel, and Anshika Aggarwal. "Advanced Encryption Techniques in Healthcare IoT: Securing Patient Data in Connected Medical Devices". Modern Dynamics: Mathematical Progressions 1, no. 2 (August 30, 2024): 224–247. Accessed October 30,2024. mathematics.moderndynamics.in/index.php/mdmp/article/view/22.