Pavani Lakshmi Mounika Ghanta

Computer Science Department

Georgia State University

pghanta2@student.gsu.edu

Iot in Healthcare

Introduction - Remote monitoring in the healthcare industry is now possible thanks to Internet of Things (IoT) enabled devices, releasing the potential to keep patients safe and healthy and enabling doctors to provide excellent treatment. As doctor-patient interactions have gotten simpler and more effective, it has also raised patient participation and satisfaction. Additionally, remote patient monitoring shortens hospital stays and avoids readmissions by keeping an eye on patients' health. IoT has a huge impact on lowering healthcare expenses and enhancing patient outcomes.
IoT is undoubtedly transforming the healthcare industry by redefining the space of devices and people interaction in delivering healthcare solutions. IoT has applications in healthcare that benefit patients, families, physicians, hospitals and insurance companies.

Using IoT for Patients Patients can access individualized care with the help of wearable devices like fitness bands and other wirelessly connected devices like blood pressure and heart rate monitor cuffs, glucometers, etc. These gadgets can be programmed to remind users to keep track of their blood pressure variations, appointments, appointments, and many other things.

As the Internet of Things (IoT) expands rapidly in the healthcare systems, such as health monitoring, fitness programs, etc., IoT-based healthcare systems are examined. IoT research projects aimed at enhancing the functionality of IoT-based healthcare systems are growing daily since variables like accuracy and power consumption are major IoT concerns. To boost device performance and handle data effectively, data management techniques in the IoT-based healthcare system with cloud capabilities are also carefully examined. The functionality of the IoT-based healthcare system, as well as its benefits and drawbacks, are discussed subsequently. The majority of research studies are effective at identifying various symptoms and can correctly forecast diseases. The IoT based healthcare system designed especially for elders is an efficient solution in monitoring their healthcare issues. Major limitations in the existing systems are high power consumption, availability of fewer resources and security issues due to the utilization of many devices. Many research works are in progress to improve accuracy, computational time and difficulties in the development.The IoT-based healthcare system uses wearables or sensors implanted in patients, both of which have relatively low battery life. The user experience is impacted by the regular charging of these gadgets and mobile devices, which might exhaust patients and involve the nurse. Monitoring heart patients is a significant and important area of research, and it is done using sensor devices.

This paper describes an existing IoT-based healthcare network and represents a summary of all prospective networks. IoT healthcare protocols are analyzed in this context and provide a broad discussion on it. It also initiates a comprehensive survey on IoT healthcare applications and services. Extensive insights into IoT healthcare security, its requirements, challenges, and privacy issues are visualized in IoT surrounding healthcare. In this review, we analyze security and privacy features consisting of data protection, network architecture, Quality of Services (QoS), app development, and continuous monitoring of healthcare that are facing difficulties in many IoT-based healthcare architectures. To mitigate the security problems, an IoT-based security architectural model has been proposed. Furthermore, this paper discloses the market opportunity that will enhance the IoT healthcare market development.

Applications of IoT devices inHealthcare:

All aspects of our lives witnessed a steady increase in Internet technology that has become ubiquitous that is infiltrating.IoT healthcare applications have the capacity to accurately track people,equipment, specimens, and supplies and can take care of various types of stakeholders, including the hospitals, diag- noses, nursing homes, and community to analyze the capturing data. Using biometrics information or measuring the important parameters from sensors to get better quality, and efficiently using the resources. To detect the misuse activation as an extreme cardio practice or accelerated exercising as analyzed to training at a methodical movement, the aforementioned data provide relevant information in the analysis and control of the diseases.

In the past decade, IoT has come a megatrend in the 4th generation revolution technologies that can offer excellent connection to each uniquely identifiable smart object and bias in Internet infrastructure.The prospect of IoT will be dominated that will serve as global programs to connect physical objects, substances, and humans and enabling new ways of working, communicating, interacting, amusing, and living. The IoT enables transforming physical objects to perform entering information and to coordinate their opinions by exercising its beginning technologies, similar as ubiquitous and pervasive computing, bedded bias, intelligence technologies, detector networks, Internet protocols(IPs), and sphere-specific operations.This paper also introduces technologies used in IOT based healthcare and also classifies the existing networks used by these devices.

The Internet- of- effects(IoT) is an exponentially adding network of physical bias(the ‘ effects ’) that contain colorful bedded seeing, recycling and communication technolo- gies to collect and communicate sensitive data through the internet All connected realities of IoT networks are responsible to collect, store, process and exchange information with each other. With the amelioration of miscellaneous technologies, IoT is rapidly proliferating in all aspects of our life. In particular, the preface of IoT operations in healthcare has the implicit to revise the sector where all the stakeholders will be connected to enable pervasive and universal healthcare for all anyhow of their locales. The integrated connectivity amongst colorful realities of a healthcare system along with the demand of accurate and timely operations means that a massive quantum of sensitive data will be involved with instant availability. A specificity of an IoT-grounded healthcare network is that the data originates at geographically distributed locales. therefore, the data is particularly vulnerable to unauthorized access and other vicious conditioning.The issue is made even more difficult by the care system for the elderly's largely physical and manual management.Additionally, the issue is being exacerbated by devices with very limited agility and communication and networking capabilities.However, the critical healthcare issue outlined above can now be addressed thanks to recent advancements in nano-bio sensors and flexible electronics. Ten years ago, this would have been unthinkable.Additionally, the rapid development of holochain-based IoT healthcare framework's ubiquitous connectivity and networking solutions, which offer a low-complexity, highly secure alternative to blockchain and mitigate security and privacy issues.The following is a list of the main benefits of using holo chain in IOT healthcare.an easy way to deal with security and privacy issues in IoT healthcare systems that is based on holochains.

Critical evaluation and comparison of the holo chain framework's advantages over blockchain-based and other existing systems.Design of systematic algorithms, procedures for validation and authentication, and holochain implementation .Framework execution examination to exhibit that our holochain based framework plan fundamentally outper-structures blockchain based arrangements as far as asset prerequisites and consequently takes care of the adaptability issue of blockchain based frameworks.

Analysis of the IoT healthcare network's security performance in comparison to blockchain and other traditional cryptographic systems.

thorough examination of the difficulties associated with holochain-based IoT healthcare systems' implementation, followed by an extensive discussion of potential future research directions.

Vulnerabilities of IOt Healthcare

Because we are increasingly relying on Internet of Things connections in all aspects of our lives, cyberattacks pose a serious threat to our day-to-day lives. This means that hackers and other malicious entities could potentially gain access to our personal data, financial information, computers and other devices, home and work data, and even medical data.There is a chance that the Internet of Things (IoT) network will be hacked or compromised.Everything that is connected to the Internet of Things network, from a heart pacemaker to our automobile infotainment, is vulnerable to cyberattacks.This is even more concerning when it comes to healthcare.

The following are a few instances in which an attacker with access to medical imagery can alter the contents to cause a misdiagnosis due to the lack of accuracy and ease with which they can hack an IOt device. In some instances, this can be fatal.The assailant can even add or remove evidence of certain medical conditions, such as injecting or removing lung cancer from a scan, adding or removing evidence of aneurysms, heart disease, blood clots, infections, arthritis, problems with cartilage, torn ligaments or tendons, tumors in the brain, heart, or spine, and other cancers. These scenarios are no longer science fiction; they are actually taking place in real life right now.We can't face challenge when it come to the existence of an individual, without legitimate determination patients might try and pass on at times because of mistake or changing of records.This is an extremely difficult vulnerability.IOT devices can be made more secure in a variety of ways, including in healthcare and elsewhere.

Architecture in IOT
A health-monitoring unit receives the data after patients are connected to sensors that are linked to control devices.Utilizing cloud technology aids in data transmission management.Because this transmission makes it possible for integrity and confidentiality to be compromised, security may then become a concern.

Hybrid Cloud Environment: A hybrid cloud architecture is proposed to simplify the IoT/Cloud architecture.Three layers make up the Service Management Framework for IoT Devices, or SMFIC:Layer for customers:collects information from patients, a social network, a smart home, and a smart healthcare service.Layer of service providers:shares physical resources, manages services, virtualizes, and offers security and privacy.Third layer:manages services between customers and service providers.

Tree of Temporal Fuzzy Ant Miners: Combines ant colony optimization, decision tree, and fuzzy rules (conditional statements) • Uses sensors to collect real-time data and examine home-based behavioral and physical trends Machine Learning Algorithm for Early Disease Detection:

A three-tier structure:Collects sensor data from wearable devices, Stores data in the cloud and provides a regression-based prediction model for heart disease. Is also used to monitor and detect arthritis Cloud Integration.The utilization of cloud technologies permits flexibility, scalability, and the utilization of a greater number of resources for the processing of the data. Patients' physiologically based characteristics are measured, and the data are saved in the cloud.Data from IoT medical devices are collected by the user subsystem and sent to the cloud subsystem for diagnosis. The network delay presents the greatest obstacle presented by this architecture.Noise will have an impact on the quality of the data as it travels from the sensor to the control device and on to the monitoring center.Improved architecture facilitates data transmission without affecting its nature.The data signal can also be improved by using a noise removal technique.

Because hackers and attackers have easy access to sensor data, IOT healthcare security is very important. We can use Non-dominated Sorting Genetic Algorithm II (NSGA-II) to optimize data access time, increase resource utilization, and reduce energy consumption while maintaining data privacy.How NSGA-II works is explained in the steps that follow.

Security in IOT Healthcare is very important aspect because Hackers and attackers have easy access to sensor data we can Optimize data access time,increase resource utilization ,reduce energy consumption these should be done while maintaining data privacy this can be achieved using Non-dominated Sorting Genetic Algorithm II (NSGA-II). The following steps explain how NSGA-II works.

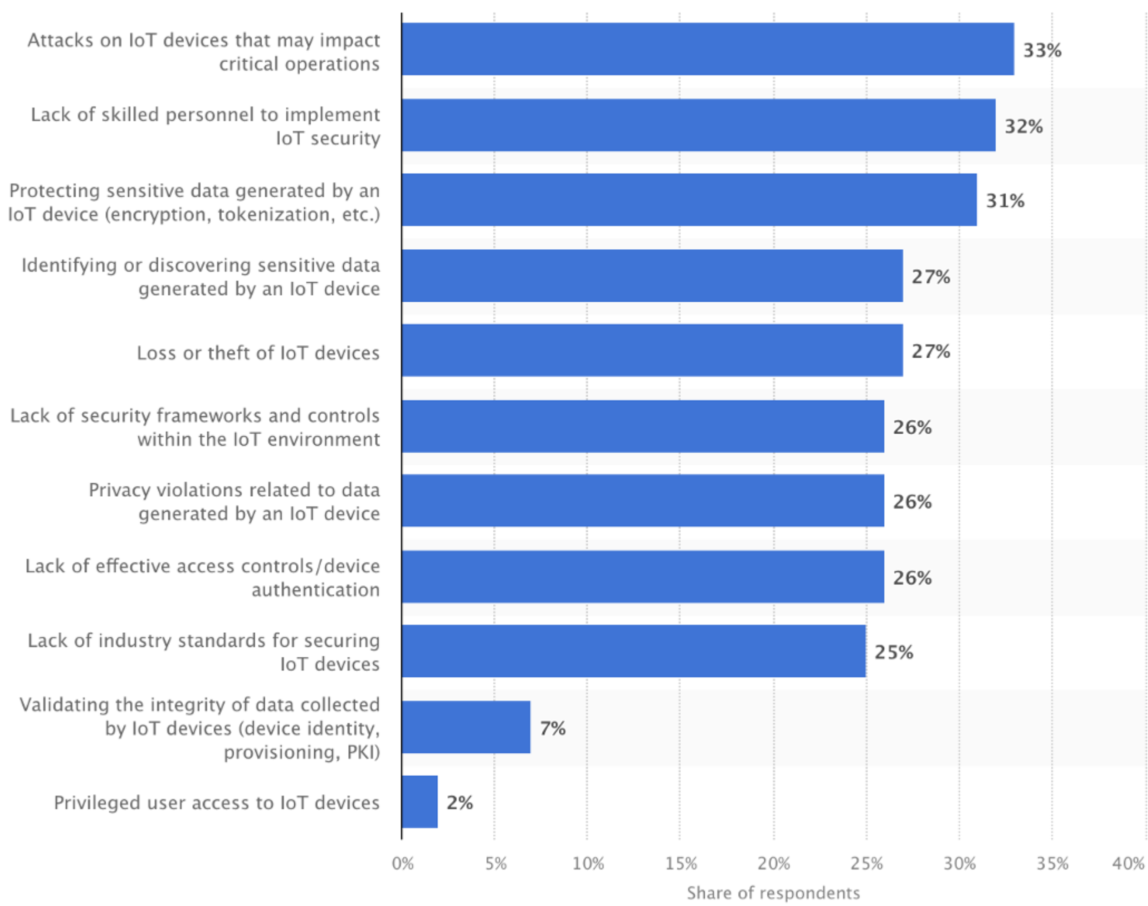
First we process data on the user's health profile and then the recommendation is processed at the cloud healthcare recommender service. After data is processed using cloud healthcare RFID encryption is used to provide security of the medical data. The Cloud Service Provider used in this algorithm has three layers. Each layer performs its task and sends the data to the next server this helps to increase security. The three layers are Authentication Server, Key Generation Center, Database Server

Theres is another secure Cryptosystem which has four phases to increase the security of the system that is Lattice-based Secure Cryptosystem
The four phases are - Setup phase, Key generation phase ,Data encryption phase, Data decryption phase. In three phases, the lattice polynomial vectors are used as input in the first phase and the KGC is generated i.e., the private and public key, in the second phase and shared with the Database Server (DS). In the last phase, the message is used as an input parameter and combines it with the random polynomial. If any user sent a request to access the medical data, the KGC transfers the secret key pair to the DS using a secure channel. The DS processes the plaintext message using the input parameters and the secret key pair.

BlockChain for IOT device security
The initial goal of using blockchain technology was to maintain massive amounts of data as a database and improve the quality of DLT.Blockchain stores data in a chain of blocks, allowing authorized users to decentralized store private or shared transactions.Blockchain's unique storage method not only provides a robust data management system but also ensures the system's data security.As a result, IoT network security could benefit from blockchain technology.Using the inherent autonomy of the holochain architecture and protocols, a holochain-based privacy-preserving secure communication scheme for distributed IoT healthcare applications has been proposed in one of the research papers.Holochain, in contrast to blockchain, runs applications (hApps) entirely on the user side, freeing the communicating agents from any form of centralized control.As a result, there is no single point of failure.Because users are the hosts, as more agents use an app, more storage and hosting power become available, lightening the load.Any agent that modifies their own app code effectively splits out of the shared DHT space and into a different application.As a result, it appears that holochain is the best technology for distributed IoT applications.The holo chain framework's significant reduction in time and space complexity in comparison to competing blockchain schemes is demonstrated by comparative performance results and analyses. This demonstrates the potential for the realistic deployment of large-scale IoT healthcare systems.

Challenges and Opportunities in IOT healthcare
Security is a crucial aspect of the Internet of Things because it is difficult to encrypt data received from low-resource devices and there is a risk of data integrity and confidentiality being compromised during data transmission from the sensor to the cloud center.Architecture for the Internet of Things with a machine learning algorithm for early heart disease detection.It has a three-tier architecture for collecting sensor data from wearable devices, storing the data in the cloud, and a regression-based heart disease prediction model.The IoT paves the way for high flexibility in IOT healthcare, i.e., the patient doesn't need to be in the hospital all the time and can live in their own home and be regularly monitored with IoT technology.Sensors and other types of wearable devices can be uncomfortable for the patient's body.Noise will have an effect on the quality of the data as it travels from the sensor to the control device and on to the monitoring center.Improved architecture facilitates data transmission without affecting its nature.Data signal enhancement can also be aided by noise removal methods.

The majority of current ECG monitoring techniques involve supervised signal analysis.This may result in a detection error and raises costs.When analyzing the signal, machine learning can be used to help cut costs and increase efficiency.Power leakage and energy consumption rise as the number of sensors and devices increases and their processing demands rise.The use of an optimization algorithm can be used to cut down on energy consumption.Storage of data in the Cloud can alleviate the storage and mainframe requirements associated with monitoring a large number of IoT users.However, the cloud-integrated Internet of Things makes things more complicated.Because the devices are more susceptible to attacks, privacy is another important issue in the Internet of Things.Encryption methods are difficult to use on these devices because of their limited resources.The management of data and the facilities for sharing resources are provided by cloud computing.Wearable technologies are effective, but users must be patient due to their short battery life cycles and frequent charging requirements (if it requires nurse participation, it kind of defeats the purpose). Additionally, the data is extremely vulnerable, making it simple for attackers or hackers to gain access to it.
Any example to understand the challenges better by looking at a survey. This survey is conducted among It employees in both technical and non technical departments where most of the attacks possible are due to lack of security in the iot devices.



Applications of IOT Healthcare:

IoT in healthcare is the ecosystem of IoT-enabled healthcare devices connected via chips, sensors, or other related technologies to constantly monitor patient vital signs (e.g. blood pressure, heart rate, temperature, respiration rate, etc.), physician's activity, and the overall hospital environment, to improve the efficiency of hospital equipment and staff.

There are many IOT Healthcare Devices, few of them are wearables like smartwatches, rings, vests, when we look into iot devices used in hospitals like monitors and sensors examples are heart monitors, sleep monitors, temperature monitors and air quality sensors. Some of the recently developed trackers like medication refill reminder technology and drug effectiveness tracking. These are few important devices used for Healthcare.

IOT Healthcare Methods
Radio Frequency Identification -Active RFID. An active RFID tag has its own power source, often a battery.Passive RFID. A passive RFID tag receives its power from the reading antenna.The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag.In healthcare, RFID technology allows the moving of medical equipment with passive RFID tags. Real-time location system (RTLS) enables real-time tracking of tagged objects and helps to create a system of connected devices that dynamically track and report any status change about their location, conditions, and amount.The RFID reader is installed in places such as medicine storerooms, check-up rooms, and sickroomsThe color of the specific RFID tag changes as a sign of disposal, disinfection, or other treatment.

Cloud computing in healthcare describes the practice of implementing remote servers accessed via the internet to store, manage and process healthcare-related data. This is in contrast to establishing an on-site data center with servers, or hosting the data on a personal computer. By using cloud computing there are many advantages Electronic Medical Record EMR collects the medical data of patients and helps to reduce data storage cost,offers superior data security, enhances patient safety, streamlines Collaborative Patient Care.The data stored can be used for medical Research. This paves the Way for Big Data Applications.

Edge Computing is a distributed computing paradigm that brings computation and data storage closer to the sources of data. This is expected to improve response times and save bandwidth.Health monitors and other wearable healthcare devices can keep an eye on chronic conditions for patients. It can save lives by instantly alerting caregivers when help is required.Robots assisting in surgery must be able to quickly analyze data in order to assist safely, quickly, and accurately. If these devices rely on transmitting data to the cloud before making decisions, the results could be fatal.

Utilizing numerous computer resources to accomplish a single objective is known as grid computing.system that allocates a group of clustered computer nodes to collaborate on a particular task.Drug discovery is one of the most technical issues that e-Health faces, and grid computing is emerging as a potential solution.Grid computing easily surpasses traditional information technology systems due to the intense real-time data throughput and the enormous demands placed on computer processing power.

A mobile grid management framework that serves as a crucial enabling technology for IoT-based, ubiquitous healthcare solutions of the next generation.IoT Healthcare Networks can be divided into three categories: IOThNet Topology, IOThNet Architecture, and IOThNet Platforms. Another study provides an overview of grid computing, discusses its potential applications, and offers a decision framework that extends the Enterprize Desktop Grid architecture to improve healthcare system decision making.

The arrangement of distinct parts is covered by the IoThNet topology.It depicts typical healthcare scenarios that specify the locations where a remote monitoring composite computing network handles a large number of vital symptoms and sensor data.The independent data were then analyzed and saved in a suitable database.It can respond according to the method, which was mentioned earlier and allows caregivers to monitor the patient's conditions from any location.In order to keep the streaming of medical data going, IoThNet topology gateways and access services also needed IP, or global system mobile (GSM).iMedPack and iMedBox are recognized in numerous wireless models as a collection of multiple sensors and interfaces, and there are related conceptual structures for healthcare applications in.Through healthcare gateways, the IoT healthcare infrastructure of topology, which integrates numerous IoT devices with clinical devices, is connected to the health-IoT cloud for data analysis and storage.

IoThNet Architecture: The IoThNet architecture's guiding principle defined the methods and functional organization of the physical elements of the IoThNet.We have explained in multiple studies that the concept of IoThNet, the sensor, and wearable data transmission over the 802.15.4 protocol have been used in IPv6 and 6LoWPAN networks.

IoThNet Platforms: The service platform in the IoT system that focuses on resident health information is the IoT healthcare network platform model.It helps to categorize the various healthcare models and the various databases that caregivers can access based on the healthcare support layer.a related concept of data platforms, such as the business layer and smart object middleware.Here, the model gets the related interoperability and the computerized plan technique ology stage coordinated for the IoT organization.It allows the IoT gateway to share support control devices by providing a variety of sensors to numerous users during the health data collection process.Health data compositions—electronic health records (EHRs)—and security systems that securely associated interoperability with the proposed structure involve multidisciplinary optimization and are applied to control management are the appliance and software interfaces established through interface standardization.

In this paper, we talk about three different IoT conventions, like application conventions, administration revelation conventions, and framework conventions.Web protocol environments limit the M2M requirements.Unrestricted security is maintained with unicast and multicast requests in UDP [RFC0768] binding.Utilizing the publish/subscribe mechanism, resource observation makes it possible to monitor the application.The client and server exchanged data using blockwise resource transport.

The CoREs' Web connection range to provide resources based on the resource discovery URI path of clients.CoAP is made possible by a proxy server using HTTP because it is compatible with certain things that are part of the standard REST architecture.The confidential message exchange is integrated with the datagram transport-layer security (DTLS) layer-creating CoAP protocol.Service Discovery Protocols The Internet of Things necessitates resource management mechanisms that are able to obtain self-configured registers and actively discover resources and services.One of the most effective and potent protocols utilized in the Internet of Things is multicast domain name system (mDNS) and DNS service discovery (DNS-SD).mDNS and DNS-SD prototypes have been designed primarily as resource-rich devices and environments, as confirmed by our analysis studies.A gathering of organized PCs which cooperate as a virtual supercomputer to perform enormous errands, for example, investigating immense arrangements of information.

Security In IOT

Security Requirements - There are many security requirements when we look at the vulnerability in the IOT device in healthcare. Some of them are common to all the IOt device few are specific to healthcare devices. Scalability ,Communications Media,Multiplicity of Devices ,Multiprotocol Network, Attacks based on Information Disruption In this security requirement we have to make sure that Interruption,Confidentiality,Modification,Replay attacks are not possible Attacks based on Host properties Here threat is on User,Hardware,Software and they might be compromised and attacker might have access to any of these components.
Confidentiality,Authentication,Availability and Integrity of user data should be maintained because it's their personal information.
Some other security Requirements are DataFreshness, NonRepudiation, Authorization, Resiliency,Fault Tolerance and Self-Healing. Self healing is specific to healthcare devices because when a IOT device implanted in a person is damaged or has some issue it has to self heal or it will affect the health of the patient. But it is hard to make these self healing devices. We should make sure that device will protect against Denial-of-Service(DoS), Unauthorized access,confidentiality of data. Making trusted platforms to share the data.

Security Challenges we face when it comes to IOt devices are restriction of computations because they have limited memory and also uncertainty in the outputs that is nothing but lack of accuracy.We have Maintain the standardization because with increasing count of IOT device it is hard to keep them up to date with the latest technologies.Interaction with Internet is important to connect the scalable networks and helps in Integrating the data and this data is managed in the cloud. Control security protocol to increase security and embedded devices with software to help in integrating the data with analyzing the health data.

Threat Model: One of the initial activities in the security engineering process is threatened by IOT. Through a threat modeling strategy that includes identifying the system architecture, threat modeling and its role in the process of risk management can be better understood.The threat model for IoT systems is based on a relatively straightforward IoT system. There are numerous security tools, technologies, and methods available to organizations with limited resources.Security benefits include incorporating threat modeling into the risk management process, as well as their effects on the system and where defensive technologies should be extended.

Attack Taxonomy The Internet of Things uses a complicated network to transfer data over the Internet.It may be necessary to embed safety-critical services and sensitive data online for the significant expansion of IoT in healthcare applications.We looked at the taxonomy of attack between IoT networks and healthcare domains, looking for information on the likelihood of security and tangible, predictable threats to support IoT developers.

Blockchain-based architectural model is a novel strategy for addressing these challenges after reviewing the various IoT healthcare security requirements, their challenges, various threat models, and attack taxonomy.

Application of IOT healthcare as discussed above we have many applications like telehealth, keeping tracking of information, drug Management, food Management. By using these devices we can determination of glucose Level, monitoring of Electrocardiogram, Blood pressure,oxygen saturation

Services of IOT Healthcare devices are Rehabilitation System,Ambient Assisted Living, m-Health .We can estimate Drug Reaction on patients and change the dosage accordingly.

Semantic Medical Access, Children Health Information, Embedded Context Prediction are few services

Security Challenges

Standardization, device security, cost, quality of service, network architecture, technology transition, power consumption, and data protection are among the challenges and unresolved issues we face. IoT Healthcare market opportunities contribute to a significant market opportunity with smart objects for machine manufacturers, application developers, and Internet service providers.Problems with M2M transportation necessitate the development of up to 45 percent of the Internet platform.On the Internet of Medical Things (IoMT), the growth of IoT is making life-enhancing progress.The most prominent commercial industries, such as Mobile Health (mHealth) and telecare, which enables preventive wellness through diagnosis, treatment, and monitoring services, will undoubtedly benefit from the impact of the IoT healthcare application.

In order to control chronic diseases like diabetes, asthma, congestive heart failure, autism, heart disease, insomnia, and BP, the Internet of Things (IoT) network in healthcare systems expands.The becoming huge measure of the IoThNet stage has given market progression a more dependable and starting examination of sickness following as referenced before.Grand View Research has also broken down the global IoT market for healthcare by end-user, utilization, element, IoThNet technology, and county.The IoT healthcare market capacity is anticipated to reach USD 534.3 billion by 2025, growing at a CAGR of 19.9% over the estimated years, according to a new report from Grand View Research.Growth in grants for connected device manufacturing solutions in the IoT healthcare sector.

Holochain for IoT healthcare's distributed security.Blockchains are made up of blocks that contain data and nodes that contain the person's transaction.Block chain's drawback is that it uses too much memory and data.Holochain eliminates the aforementioned flaw.By storing essential data in the nodes, Holochain saves time and memory compared to blockchain.They are better at avoiding attacks they don't want.When it comes to large networks, holochain is more effective than block chain and costs less to maintain. The structure of holo chain is DNA, Genesis, and Transactions.where Holochain's overall structure is made up of DNA.A hash is included in Genesis to guarantee that the DNA blocks adhere to the rules.Additionally, it creates a happ with the necessary code.To support the hosts, Holofuel deals with online currency.Hash Chain ensures none of the information gets changed.DHT is a network in which users can send data through nodes.

Holochain's advantages over block chain include the potential to conserve healthcare system resources and time.There are still risks, like DDoS attacks, data manipulation with malicious intent, and MitM. Holochain will eventually take over the healthcare industry.

Holochain:Security arrangements give better versatility and have diminished network traffic,low-intricacy exchange approval.Because Holochain has an effective consensus mechanism, it is more resistant to consensus-based attacks.They can also generate application-dependent validation functions and offer solutions at a reasonable cost.

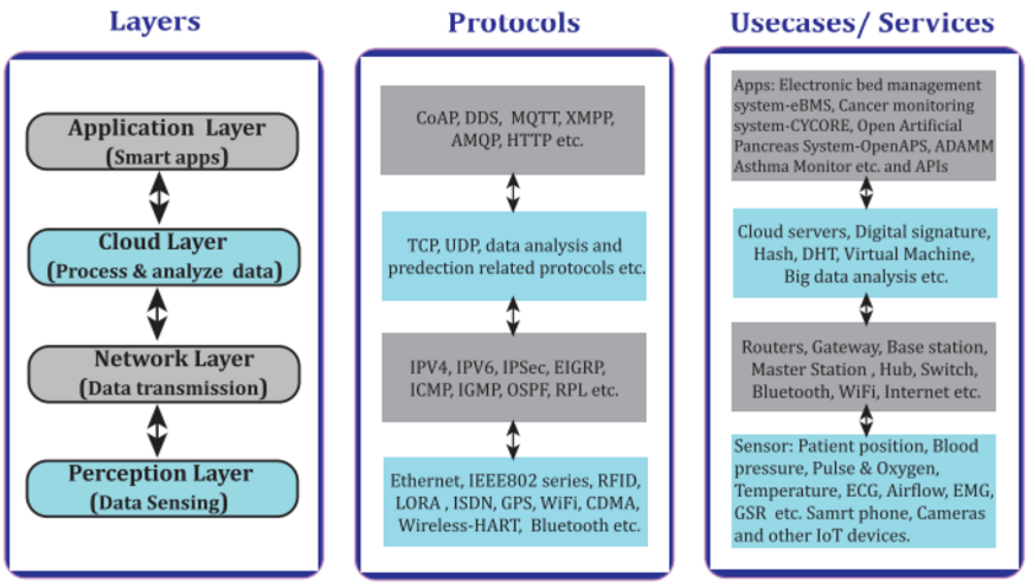


FIGURE 3. Layer-wise protocols and technologies of the IoT healthcare architecture.

Holochain-based IOt healthcare model: The layer and the tasks performed at that layer are depicted in this figure.When implementing this technology, the security threats we face include unauthorized access, illegal or intentional data tampering, MitM, DoS double spending attack, and protection against these attacks. Key components include the holochain, holo fuel, hash chain, DHT, and source chain structure.

This article uses the inherent autonomy of the holochain architecture and protocols to propose a privacy-preserving, secure communication scheme for distributed IoT healthcare applications.Holochain, in contrast to blockchain, runs applications (hApps) entirely on the user side, freeing the communicating agents from any form of centralized control.As a result, there is no single point of failure.Because users are the hosts, as more agents use an app, more storage and hosting power become available, lightening the load.Any agent that modifies their own app code effectively splits out of the shared DHT space and into a different application.As a result, it appears that holochain is the best technology for distributed IoT applications.The holo chain framework's significant reduction in time and space complexity in comparison to competing blockchain schemes is demonstrated by comparative performance results and analyses. This demonstrates the potential for the realistic deployment of large-scale IoT healthcare systems.

Conclusion:

ECG monitoring system that can easily predict disease symptoms using machine learning.Due to the limited storage space required for some encryption methods, privacy is the primary concern in the Internet of Things.The advancement of healthcare systems as a result of the incorporation of IoT technologies is reshaping the sector's future. Cloud storage facilitates the handling of large amounts of data generated by the system and increases its complexity when combined with the Internet of Things.We have talked about the general security requirements of an IoT system and the typical obstacles to meeting those requirements in this section.Additionally, we explained a Blockchain-based top-level architecture for an IoT system that can address current security issues.After that, we talked about the applications and services where IoT has a big impact on the healthcare industry.We included the difficulties and unresolved issues that the Internet of Things (IoT) still faces as well as the opportunities that remain in the healthcare market as integral parts of our evaluation.

By bringing their cutting-edge concepts, cutting-edge implements, and cutting-edge software to market, researchers all over the world are working tirelessly to enhance the healthcare system.The protocols, architectures, and platforms of various contemporary IoT networks were the primary focus of this review.Information on IoT healthcare research activities related to private health, elderly monitoring, and chronic disease supervision was provided in this article.Security, privacy, authentication, energy consumption, computation power, resource management, quality of service (QoS), and other key issues with IoT healthcare systems are discussed in depth here.This report uses the inherent autonomy of the holochain architecture and protocols to propose a privacy-preserving, secure communication scheme for distributed IoT healthcare applications.

Reference:

https://www.prweb.com/releases/2018/02/prweb15236189.htm
https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/#:~:text=IoT%20has%20applications%20in%20healthcare,rate%20monitoring%20cuffs%2C%20glucometer%20etc.

Three topic 5 papers uploaded in icollege