Review And Analysis On Security And Privacy In Healthcare IoT Investigate The Security And Privacy Challenges Posed By The Widespread Adoption Of IoT Devices In Healthcare

[1] Mounika Nalluri, [2]Manideep Yenugula, [3]Aruna Sri Rongali, [4] Chinna babu Mupparaju

[1] Senior Software Engineer, Information Technology(Masters in Computer Information Systems), Murray State University, USA,
[2] Senior Performance engineer, Computer science , Chickasaw nations, Dallas, TX,
[3]Senior Software engineer, Graduate Doctoral Information Technology/Graduate (Information Technology Emphasis/Information Technology, Ph.D.), University of the Cumberlands, St.Louis, MO,
[4]Software Engineer, Information Technology(Masters in Computer Science), University of Central Missouri, USA,

E-mail: mounikanalluri89@gmail.com, [2]manideepyenugula@ieee.org
[3]arongali34683@ucumberlands.edu, [4]chinnababumupparaju@gmail.com

Abstract: E-Health refers to the utilization of the Internet and other interconnected networks in healthcare systems. In this work, we analyzed research papers that were conducted between 2017 and 2020. Our aim was to examine the evolution of intelligent techniques in healthcare and their use throughout time, paying special attention to the integration of IoT devices and cloud computing. "Seek, find, understand, and appraise health information derived from electronic sources and acquired knowledge to properly solve or treat health problems" is what E-Health measures. The abundance of health information and e-Health analysis accessible online enables consumers to safeguard themselves and make empowered decisions regarding their health. False information is less likely to be found online when e-Health is heavily integrated. Several viewpoints on privacy and security in IoT-based cloud-based e-Health systems are discussed in this article, which also lists the pros, cons, and future possibilities of implementing such systems. Integrating intelligent technologies like cloud computing with IoT-based electronic health records systems allows for the creation of smart objectives and applications. The future looks bright for this trend.

1. Introduction

The rising tide of high-profile hacks throughout the country suggests that security breaches are becoming more common and more damaging. Information security breaches and cyberattacks are listed as one of the top five worldwide hazards in the 2019 "World Economic Forum global" risk report [1]. These threats are now seen as paramount, just as last year. An enormous ransomware attack recently disrupted and delayed services in various departments, adversely impacting several healthcare organisations. Risk to patients' well-being was posed. Figure 1 shows the number of data breaches and exposed records in the US from 2005 to 2019.

A lot of effort is going into the healthcare industry's efforts to give patients the personalized treatment they're used to in other parts of their lives. On the other hand, they are already facing significant challenges due to the plethora of new issues that are emerging in the healthcare industry. Healthcare costs are on the rise, data security is a concern, there is a lack of qualified staff, the population is getting older, new infectious diseases are emerging, and everyday health issues that were previously unknown are being discovered, among other global challenges that are impacting the medical industry [2, 3]. Contactless and remote monitoring of the elderly through Internet of Things-based systems has the potential to improve clinical outcomes, save expenses, and increase the productivity of healthcare workers [4]. As a result of the IoT, healthcare providers and other carers can access a patient's vital signs, test results, medical history, and prescription information remotely or from any place using a mobile device. It is also possible to advise and monitor patients remotely [5]. Securely recording patient health information from numerous sensors is the goal of IoT-based solutions. In the long run, sophisticated algorithms can be used to evaluate the data, and then it can be shared wirelessly with doctors who can subsequently provide appropriate health advice. Commonplace Internet of Things (IoT) devices in healthcare include implanted heart monitors and infusion pumps, which can administer a patient's blood with a predetermined amount of fluids, drugs, or nutrients. Along with pacemakers, insulin pumps, and cochlear implants, there are millions of other Internet-connected gadgets accessible. Not all of these devices can receive and send data; some, like the pacemaker, can only transfer data over a wireless link. Your heart rate, the stages of your sleep cycle, and the amount of steps you take or calories burned can all be recorded by wearable devices like the Fitbit, Apple Watch, smart bracelets, or smart rings. At this stage, the data is synchronized with the wearable device in order to track the monitored person and conduct further data analysis [6].

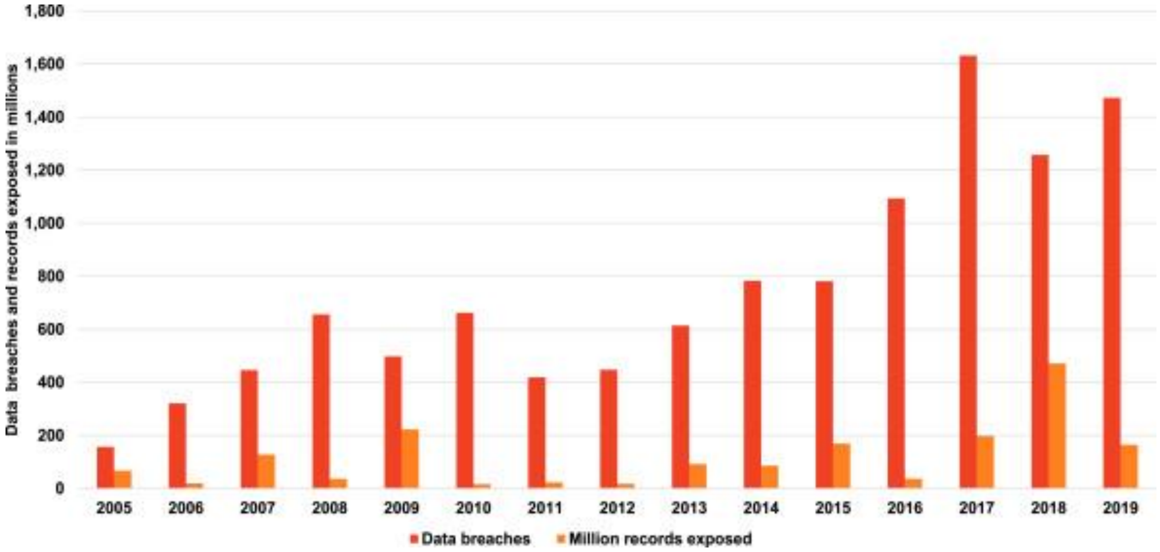

Fig. 1. Data breaches and exposed records in the US per year from 2005 to 2019.

1.1 Resource Center for Identifying Theft

These devices are useful because they allow people to keep tabs on multiple factors from the comfort of their own homes without interfering with their routines. On top of that, they may track patterns in physiological data over time and instantly notify medical staff or caretakers of an emergency, like a fall in the elderly [7]. Pharmaceutical businesses can streamline clinical trial procedures with the use of internet-of-things-based wearable gear that improves data collection [4]. The latest predictions from "World Population Prospects 2019" put the global population at 8.5 billion in 2030, 9.7 billion in 2050, and 10.9 billion in 2100. On a more critical note, the number of those 65 and older will surpass the number of people aged 15–24 by 2050, reaching 1.5 billion. Additionally, individuals are worried about the healthcare expenditures that are anticipated to increase at a frightening pace. The health care industry ate up 7.5 trillion US dollars in 2016, or 10% of GDP. At 8.2% of GDP, health care is the most expensive sector in high-income nations. The health sector accounts for a smaller proportion of GDP (6.3% in low and middle-income nations) [8].

The expansion of Internet of Things (IoT) technologies has led to a greater incorporation of technology into people's daily lives. There will be a massive influx of employee data collected and analysed, including their health status, activities, and more. Not only are there more threats, weaknesses, and bad actors in the cyber world, but technology is also getting more intuitively sensitive, which means it might affect every part of people's lives.

This study has two important contributions. To start, we draw attention to the fact that healthcare IoT devices are fraught with privacy and security risks. Secondly, we provide some ideas on how to stop or lessen the impact of such hostile efforts by using certain processes or approaches. Based on the methods and approaches suggested by security experts, we expect this to direct future studies that employ and apply tangible solutions for healthcare issues related to the Internet of Things (IoT).

2. Literature Review

Users' data is no longer protected from a variety of threats, including spoofing, jammer attacks, and other forms of illegal access, as mentioned by the authors in [9].Potential solutions exist to assist individuals in securing their IoT devices through the implementation of various security procedures.

According to [10], there are a slew of recently found privacy issues that could affect the IoT and its integrated network. Organizational and business-level security management of IoT devices is challengingBusinesses should install scanning and monitoring software on all of their IoT devices to find any privacy threats and try to reduce the chance of a breach. A variety of cyber hazards can be detected and investigated with the use of traffic analyzers and interceptors.

The present state of IoT security has been the subject of numerous studies and services [11]. Numerous new dangers have emerged targeting the Internet of Things (IoT) and the security measures it utilizes. The utilization of various simulation tools, modelers, and platforms capable of verifying protocols can be beneficial for building protocols for creative IoT security. A plethora of simulation tools and modellers have allowed investigations into the security of the IoT to advance rapidly. In the event that the Internet of Things devices malfunction, it will cause significant issues.

The writers of [12] hold the view that, while the many advantages enjoyed by users, the Internet of Things is not without its share of problems that must be addressed. Most people are worried about privacy and cybersecurity. Many public and private entities are in a huge jam because of these two. The hackability of the Internet of Things (IoT) has been proven by multiple high-profile incidents. This is due to the fact that connecting networks in the IoT opens the door to the open and untrusted Internet, necessitating extra security precautions. During the implementation of the IoT security system, it is crucial to highlight the principles and standards of the IoT Cyber Security Framework.

An essential initial step, as stated in [13], is to terminate a contract including devices that use several communication protocols. Important parts of any IoT cybersecurity architecture—individual service contracts—cannot be executed due to protocol differences. He proved that certain little adjustments are necessary to lessen the dangers to IoT cybersecurity, which is crucial for assuring the IoT framework's dependability in this area.

As shown in [14], scalability is another crucial criterion for measuring the performance of the cybersecurity Internet of Things framework. According to experts, there should be no more than one billion Internet-related and cybersecurity-related problems that the IoT environment can't manage. Furthermore, the magazine demonstrated that in order to effectively mitigate risks and difficulties, the cybersecurity environment for the Internet of Things (IoT) should also facilitate testability.

In [15], the authors laid up a number of comparable cybersecurity solutions for the IoT. Since it is not in the supplier's financial interest to create high-quality solutions, they have instituted certain fundamental security measures. There is little hope that businesses will discover a foolproof method to address the cybersecurity issue plaguing the Internet of Things.

In addition, essential infrastructure, contemporary automobiles, and industrial control systems are all currently embedded with mobile and cyber-physical systems, according to the authors in [16]. With their robust connectivity and effective utilisation of new generations of embedded devices, contemporary initiatives and trends like Industry 4.0 and the Internet of Things (IoT) show the possibility of new user experiences and distinctive business models. These systems produce, analyse, and transfer vast amounts of useful data. Internet of Things systems are a prime target for cybercriminals because of the personal data and sensitive information they contain, putting people's physical safety at risk and interfering with their daily lives. Cybersecurity and privacy are two pressing issues that need serious thought because of the risks they pose. New dangers to interconnected industrial IoT networks arise from the intricacy of these systems and the possible consequences of cyberattacks. When it comes to privacy and security, industrial IoT systems can benefit from broad security frameworks. These days, IoT solutions just can't handle all the things that need to be secured.

Therefore, it has been very important to investigate and research various IoT security challenges. One of the primary goals of Internet of Things (IoT) security is to guarantee the availability of the ecosystem's many services while also ensuring user safety and anonymity. Therefore, different computer platforms and a plethora of modeling tools are providing the necessary push for study into various facets of IoT security [17].

3. System Model And HIOT Technical Requirements

A. System Model

Healthcare goods, services, and patient-centered, individualized therapies are greatly improved by HIoT. The vast majority of products designed with patients in mind have sensors or microchips built in. As shown in Figure 2, a smart healthcare system typically has a three-tier architecture.

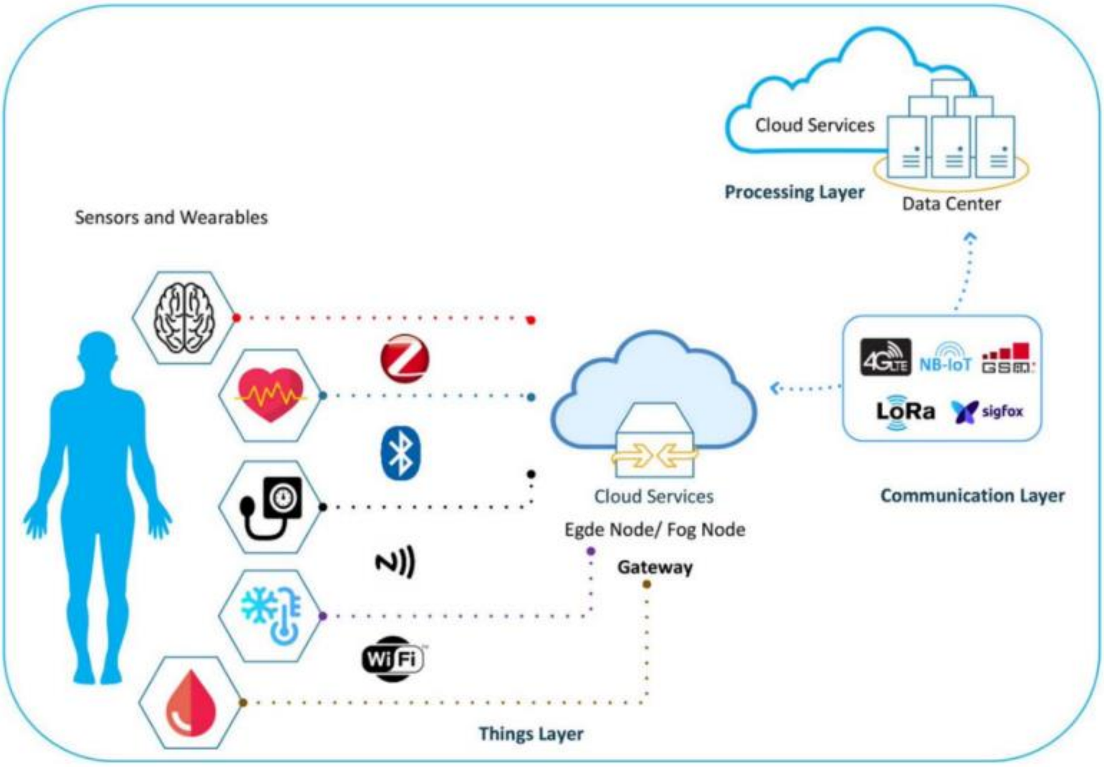

Fig. 2. The Internet of Things (IoT) healthcare system's three-tier design

TABLE I. HEALTHCARE IOT (HIOT) FUNCTIONALITIES

Remote health monitoring	Help the doctors and healthcare workers remotely monitor the patient's health. Data collected from remote monitoring devices help medical workers respond to emergencies, analyze patient health, prescribe context-based personalized medication, and update suppliers about patient needs. Examples include respiratory and asthma monitors, heart rate monitors, and insulin monitors.
Body wearables devices for self-assistance and monitoring	Assist patients and the medical team constantly comprehend the health condition, monitor health remotely, individuals take precautions based on wearable gadget readings, and medical team and care workers respond to emergencies. Examples include fitness trackers, heart rate trackers other health monitoring devices.
Personalized patient medicine infusing	The demand and supply of medication can be automated using patient-focused medicines. This is implemented using wearable IoT devices. An example includes IoT enabled insulin infusers and IoT based asthma inhalers.
Maintenance of medical equipment	The efficient maintenance of medical equipment saves lives and money. The data collected, faults reported, and track of usage help the maintenance team provide support in advance effectively.
Medical asset management	Beds, medical equipment and other assets must be easily trackable to respond to emergencies, reduce cost on asset management, and to provide a better medical care experience to patients.

Interconnected sensors and gadgets A gateway receives data from medical devices by WiFi, Bluetooth, or Zigbee, and then processes it using cloud services and edge or node computing. The processing layer is responsible for transmitting data to the data centre via wide-area communication technologies including NB-IoT, 4G LTE, and LoRaWAN. Before any of this massive data is made available to any patient, it is processed and analysed at the data centre. On top of that, you can find the essential features of an HIoT in Table II. The authors' stated intention to centre the research on a remote patient monitoring system is clear from the study's scope. Ensuring the privacy and security of patient healthcare data and the Internet of Things infrastructure is of the utmost importance. Many security breaches in smart healthcare systems have occurred because the security architecture was disregarded, which is caused by the processing capabilities, restricted power, and other restrictions of the IoT devices.

B. Technical Requirements and Challenges

Internet of Things (IoT) devices for healthcare and wireless medical sensor networks are becoming increasingly important to healthcare systems. Strong authentication, authorization procedures, configuration constraints, encryption, and the usage of standard protocols are required for the protection of static and dynamic sensitive personal information that devices collect and to prevent unauthorised access. On the other hand, worries over the safety and confidentiality of user information have not been sufficiently addressed by the IoT.

Devices that connect to HIoT network systems through several channels provide the greatest obstacle to healthcare IoT (HIoT) security solutions. Consider the BYOD initiative as an example of a gadget that contributes to the HIoT. The capabilities and operating systems of IoT devices differ from those of traditional systems. Strong passwords, authentication methods, encryption, up-to-date firmware, and software are some of the common security protections that these devices could lack. Security risks to the entire network can be posed by integrating these devices with smart healthcare systems and IoT networks. Medical infusion devices have security flaws that could compromise patient safety, hospital networks, and medical data, according to experts in cyber and internet of things network security. Without encryption or passwords, a multitude of diverse gadgets are linked to the internet through hospital networks. Attackers could steal data, target specific devices to disable them and eliminate potentially life-saving features, or conduct a mass attack on a certain type of device

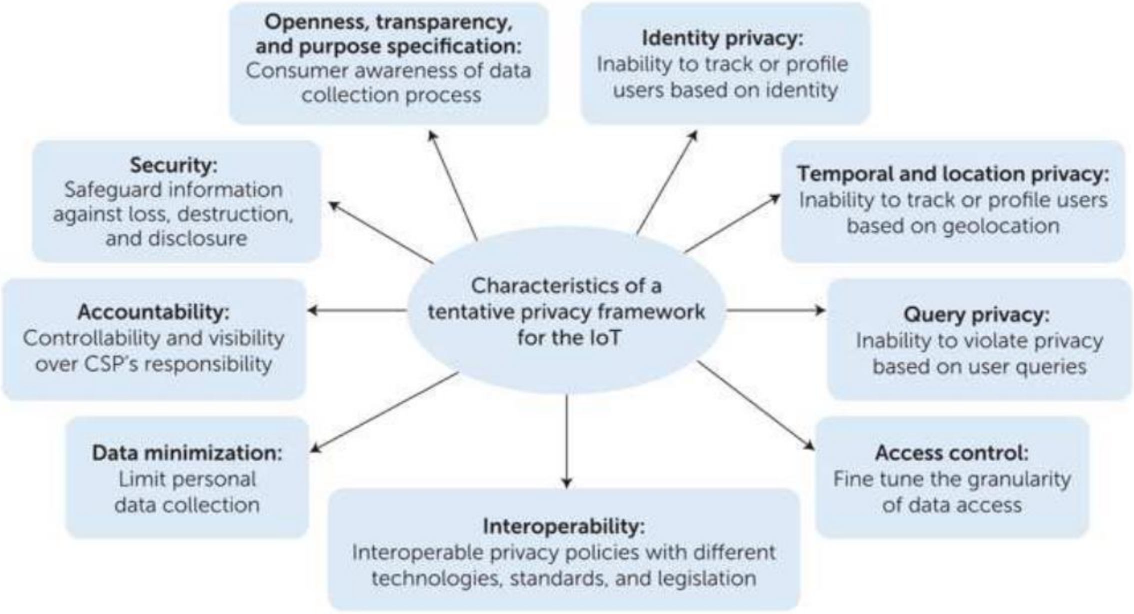
Openness, transparency, and purpose specification: Consumer awareness of data collection process
Identity privacy: Inability to track or profile users based on identity
Security: Safeguard information against loss, destruction, and disclosure
Temporal and location privacy: Inability to track or profile users based on geolocation
Characteristics of a tentative privacy framework for the IoT
Accountability: Controllability and visibility over CSP's responsibility
Query privacy: Inability to violate privacy based on user queries
Data minimization: Limit personal data collection
Access control: Fine tune the granularity of data access
Interoperability: Interoperable privacy policies with different technologies, standards, and legislation

Fig. 3. Features of the security architecture for Internet of Things solutions

Figure 3 shows the study's suggestions for a preliminary privacy framework for IoT applications. The authors are of the opinion that privacy risks and assaults are inevitable as a result of the interdependence of ISPs and cloud service providers in the transit and storage of user data. One of the most important aspects of the HIoT is remote health monitoring, which makes use of the relatively high availability and accessibility of user data. Because of this, users and patients are more vulnerable to privacy concerns, necessitating the implementation of stronger privacy frameworks. Most often used with WSN are scenario-based privacy-enhancing technologies (PETs) and the underlying technology.Protecting WSNs from both internal and external privacy assaults is the job of privacy solutions based on cryptography. But sophisticated cryptographic methods might drain WSN's resources and power supply, and assaults with a high computing power could succeed [18].

4. Proposed IoT Layered Models

We present a fresh perspective on Internet of Things (IoT) models that is both generic and extensible, with the goal of identifying and separating layers and components related to privacy and security. In order to put these proposed IoT models into action, we developed an IoT solution that has both cloud and edge support. To begin, we provide an overview of the generic and stretched models; next, we detail our experimental setup and environment for implementing the models (layered model implementation); and lastly, we present and discuss the results.

4.1. Generic IoT Layers and Data Fusion Model

Figure 4 shows the three main components of the Internet of Things model: devices, clouds, and end-users. The authors are unaware of any other works that deal with comparable ideas. Wireless sensor devices with Internet connectivity, data-gathering electronics, and communication protocols make up the device layer. These components transfer data to a storage area, either locally or remotely, for subsequent processing. With these gadgets, the user can adjust the collection frequency to acquire data in real-time. Sensor data can be stored and processed, noise removed, features extracted, and data massaged in the cloud. A decision support system employs AI and complicated data processing to use this information to make a health-related choice. The end-user layer, which encompasses the receiver, could take many shapes. It is deeply worrisome that smart devices may have security and privacy issues. The decision support system's robustness is ensured by placing multiple sublayers or modules within these three layers. A fantastic approach to guarantee data transmission and processing speed, particularly for time-sensitive decisions, is to implement an edge computing capability that can make intelligent decisions, store a replica of the data, and transmit it to the cloud for processing and long-term storage. There may come a time when specific wearable gadgets require an upgrade to their acquisition rate or capability, which will call for new security protocols to be put in place.

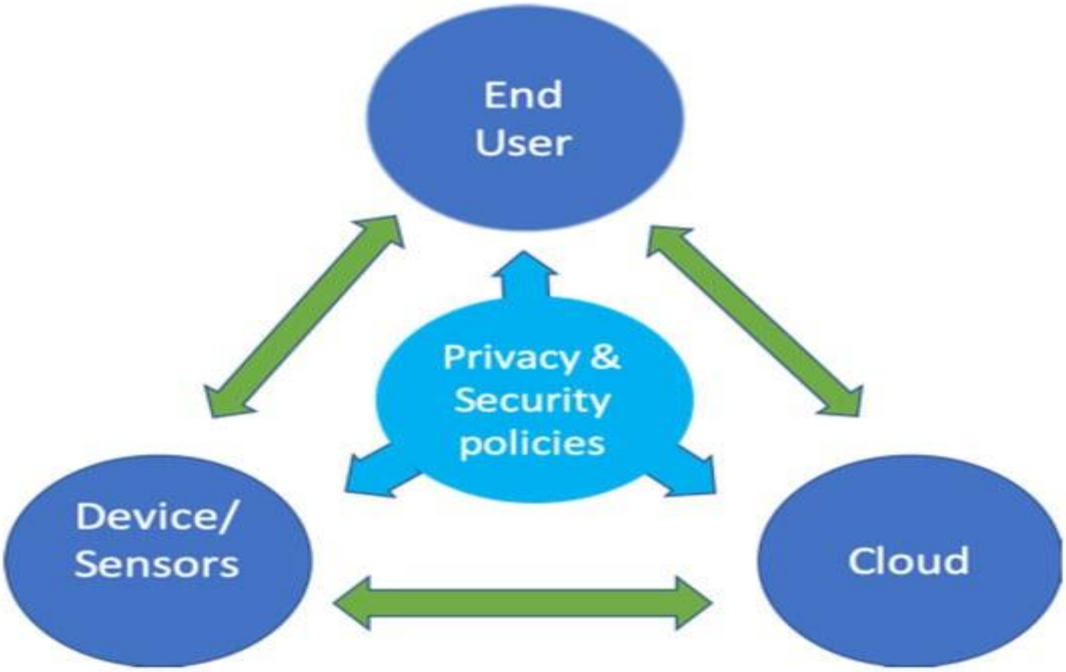

Figure 4. Security and privacy requirements for the IoT standard model.

Figure 5 displays the generic model in its original, undistorted form. You have excellent visibility into the recently introduced fog and edge layers. Faster decision-making and elimination of latency are benefits of using both levels independently of cloud-based services. As soon as a sensor connects to or is physically near another device, edge computing takes place on that device. In addition to facilitating administration and decision-making in real-time across data sources, these levels also facilitate data transmission for analytics, storage, and fusion via communication with other layers. By virtue of the fog computing layer, processes at the edge of a network leverage a more powerful computer resource that is geographically far from the sensors and data sources but still linked to the local area network [19]. Additional security and privacy concerns are spawned by these supplementary advantages.

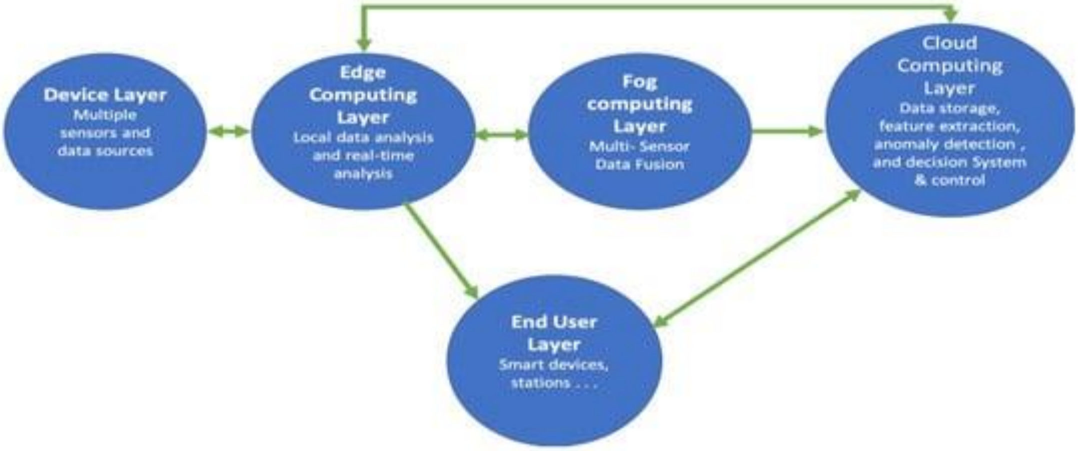
Device Layer
Multiple sensors and data sources
Edge Computing Layer
Local data analysis and real-time analysis
Fog computing Layer
Multi- Sensor Data Fusion
Cloud Computing Layer
Data storage, feature extraction, anomaly detection , and decision System & control
End User Layer
Smart devices, stations . . .

Figure 5. IoT stretched model.

4.2. Security and Privacy Policies

In order to store, process, and share data, cloud computing is a crucial component of the IoT infrastructure [20-23]. The Internet of Things' data storage and communication nodes and devices are easy prey for cybercriminals. When cybercriminals get access to sensitive patient data or electronic medical records, they launch a coordinated assault on healthcare institutions. The IoT paradigm's multi-tiered structure offers new opportunities to strengthen privacy and security while simultaneously increasing risks to preexisting ones. To reduce the risk of these types of attacks, procedures like as permission and certificates that trust particular servers must be implemented at the device layer before data from sensors is transferred to the cloud, fog, and ultimately the edge. The power consumption is an issue because some wirelessly enabled devices, like wearables, are battery operated; however, firmware and hardware address authentication and other concerns. Achieving security and power constraints will necessitate a revisit of such security measures. On the cloud layer, security protocols must be guaranteed between fog nodes and edge nodes, and on occasion, from sensors. Encryption techniques that make it harder to eavesdrop or record data include message passing protocol, point-to-point encryption, and certificates. Health systems should update their service certificates and ensure compliance with HIPPA standards to prevent SQL injections, sniffer, and phishing scripting attacks [24-28]. Because it gives hackers more ways to identify users, data fusion makes people worry about their privacy. Conventional security measures are rendered ineffective when considering the potential entry and exit of IoT devices into the sensor and data source network. This highlights the necessity for innovative, smart, and flexible security methods [29-30].

5. Conclusions

Internet of Things (IoT) devices and apps are becoming indispensable in today's world. Providing us with safe and convenient services whenever we need them, IoT gadgets are popping up all over the place, from our homes and workplaces to public spaces like schools, malls, and airports.

Stakeholders are able to collaborate more easily and gain insight into company needs and results thanks to IoT-connected devices. Furthermore, industrial infrastructure efficiency and production can be enhanced by data processing and analytics enabled by the Internet of Things.

Also, many different kinds of helpful technological developments are being implemented by IoT systems in different industries. In order to safeguard their linked devices against harmful assaults, numerous suppliers and businesses implement a multitude of policies. There has been an upsurge in reports of privacy and security issues due to the proliferation of these devices linked to both public and private networks. Some say that our coffee makers are listening in on our conversations, while others claim that our smart doorbells are providing government authorities with images of our guests. The seriousness of the security risks connected with Internet of Things devices is demonstrated by numerous real-world instances. With trillions of devices, lives, data, and privacy at stake, HIoT is an essential Internet of Things application. This sector of the economy is worth millions of dollars and has the potential to save even more.

References

[1] World Economic Forum World economic forum: Global risks report 2019 Comput. Fraud Secur., 2019 (2) (2019), p. 4, 10.1016/S1361-3723(19)30016-8 URL: http://www.sciencedirect.com/science/article/pii/S1361372319300168 View article Google Scholar

[2] Blendon, Robert J. C.D. Future health care challenges Issues Sci. Technol., 4 (19) (2003) URL: https://issues.org/blendon/ Google Scholar

[3] Sadek I., Demarasse A., Mokhtari M. Internet of things for sleep tracking: wearables vs. nonwearables Health Technol. (2019), 10.1007/s12553-019-00318-3 View article Google Scholar

[4] Minoli D., Sohraby K., Occhiogrosso B. IoT security (IoTSec) mechanisms for e-Health and ambient assisted living applications 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE (2017), pp. 13-18, 10.1109/CHASE.2017.53 View article View in ScopusGoogle Scholar

[5] Dimitrov D.V. Medical internet of things and big data in healthcare Healthc. Inform. Res., 22 (3) (2016), pp. 156-163, 10.4258/hir.2016.22.3.156 View article View in ScopusGoogle Scholar

[6] Chacko A., Hayajneh T. Security and privacy issues with IoT in healthcare EAI Endorsed Transactions on Pervasive Health and Technology, Vol. 4, EAI (2018), 10.4108/eai.13-7-2018.155079 View article Google Scholar

[7] Korhonen I., Parkka J., Van Gils M. Health monitoring in the home of the future IEEE Eng. Med. Biol. Mag., 22 (3) (2003), pp. 66-73, 10.1109/MEMB.2003.1213628 View article View in ScopusGoogle Scholar

[8] World Health Organization I. Public Spending on Health: a Closer Look at Global Trends: Technical documents World Health Organization (2018), p. 56

[9] Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wirel. Commun.* **2018**, *25*, 53–59. [**Google Scholar**] [**CrossRef**]

[10] Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30. [**Google Scholar**]

[11] Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [**Google Scholar**]

[12] Leloglu, E. A review of security concerns in Internet of Things. *J. Comput. Commun.* **2016**, *5*, 121–136. [**Google Scholar**] [**CrossRef**][**Green Version**]

[13] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. *Future Internet* **2017**, *9*, 27. [**Google Scholar**] [**CrossRef**][**Green Version**]

[14] Ali, S.; Bosche, A.; Ford, F. *Cybersecurity Is the Key to Unlocking Demand in the Internet of Things*; Bain and Company: Boston, MA, USA, 2018. [**Google Scholar**]

[15] Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6. [**Google Scholar**]

[16] Izzat, A.; Chuck, E.; Lo'ai, T. *The NICE Cyber Security Framework, Cyber Security Management*; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5.

[17] Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*; Wiley: West Sussex, UK, 2017; pp. 243–261

[18] Karunarathne, S M, Saxena, N. and Khan, M K 2021. Security and privacy in IoT smart healthcare. IEEE Internet Computing 25 (4) , pp. 37-48. 10.1109/MIC.2021.3051675

[19] Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [**Google Scholar**] [**CrossRef**]

[20] Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eyers, D.M. Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 269–284. [**Google Scholar**] [**CrossRef**][**Green Version**]

[21] The HIPAA Privacy Rule. Available online: **https://www.hhs.gov/hipaa/for-professionals/privacy/index.html** (accessed on 19 October 2019).

[22] Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 2015. Available online: **http://jolt.richmond.edu/v21i2/article6.pdf** (accessed on 6 March 2020).

[23]Ramya Thatikonda, Bibhu Dash, Meraj Farheen Ansari, Srinivas Aditya Vaddadi, E-Business Trends and Challenges in the Modern Digital Enterprises in Asia, Digital Natives as a Disruptive Force in Asian Businesses and Societies, Pp 22-43.

[24] Santosh Vishwakarma, Rajat Subhra Goswami, P Prathap Nayudu, Krovi Raja Sekhar, Pandu Ranga Rao Arnepalli, Ramya Thatikonda, Wael MF Abdel-Rehim, Secure federated learning architecture for fuzzy classifier in healthcare environment, Soft Computing, Pp 1-12, 2023

[25] Naga Simhadri, TNVR Swamy, Awareness among teaching on Artificial Intelligence (AI) and Machine learning (ML) applications based on fuzzy in education sector at USA, Soft Computing, Pages 1-9, 2023.

[26] N Simhadri Apparao Polireddi, J Kavitha, Effectiveness of automated chatbots for operational support and self-service based on fuzzy classifier for ASD, Soft Computing, Pages 1-8. 2023.

[27] R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.

[28] R Pulimamidi, P Ravichandran, Connected Health: Revolutionizing Patient Care Through Artificial Intelligence Innovations, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 3940-3947.

[29] R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.

[30] GP Buddha, SP Kumar, CMR Reddy, Electronic system for authorization and use of cross-linked resource instruments, US Patent App. 17/203,879.