Internet of Things in Healthcare

Rahul Goyal, Ruchi Sharma

Department of Computer Applications,
Chandigarh School of Business, Jhanjeri
Mohali
officialrahulgoyal26@gmail.com

ruchi478@gmail.com

Abstract

The health monitoring system plays a pivotal role in healthcare management. Internet of Things (IoT) technology is an emerging field that facilitates the connectivity of devices to the internet. Consequently, patient data can be transmitted to the cloud for accessibility via the internet, enabling doctors to remotely monitor patients and vice versa. This paper explores the services and applications of IoT in the context of health monitoring systems, while also addressing key challenges. Given the sensitive nature of patient health data, encryption techniques for data protection are also examined.

Keywords—*Challenges in IoT, Data protection, Encryption, IoT technology, IoMT*.

I. Introduction

In the contemporary world, there are five rapidly advancing technologies: the Internet of Things (IoT), 5G, cloud computing, artificial intelligence (AI), blockchain, and distributed ledger technology. Our primary focus here is on IoT. Simply put, IoT refers to the technology where devices are interconnected via the internet to a virtual platform. It enables real-time data acquisition, transfer, device connectivity, and control of end-user applications. With the rapid progress in web innovation and communication technology, our daily routines are increasingly centered around the virtual realm. [1]

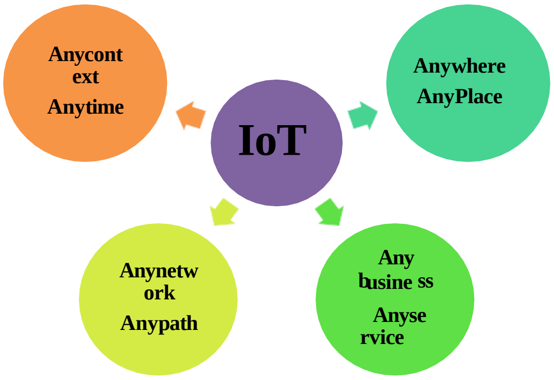

Fig.1 Brief overview of definition of Internet of Things

In the context of healthcare, the term Internet of Medical Things (IoMT) is commonly used. IoMT pertains to healthcare applications that involve interconnected devices capable of sensing critical human physiological data in real time. The IoT holds significant promise in healthcare, empowering patients to manage their own illnesses and seek assistance during emergencies using portable devices.[2].

The demand for personalized healthcare assistance is expected to rise swiftly. The integration of IoT into health monitoring systems through mobile phones is known as M-HEALTH. It encompasses data sensing, analysis, and storage from various sources, such as devices, biomedical sensors, or medical diagnostic systems. However, many of these devices, systems, and applications lack adequate measures to address security and privacy attacks, leading to numerous security and protection issues within IoT systems. Examples include concerns related to access control, authentication, and privacy breaches. [3]

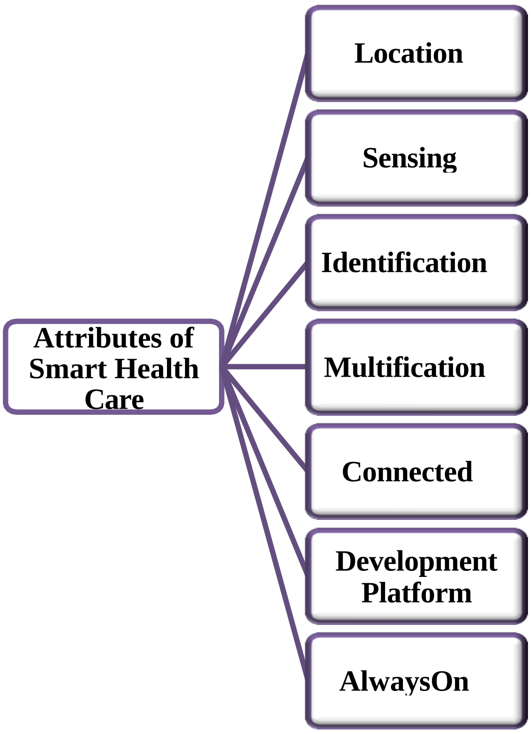

Fig.2Attributes of Smart HealthCare

II. Literature **Survey**

A. Alasmari and colleagues [4] (Alasmari et al., 2019) emphasize the importance of safeguarding patients' sensitive data and delve into the challenges and investigations concerning security and protection within IoT frameworks.

B. Farooq (Farooq, 2020) [11] provides a comprehensive overview of the IoT landscape, examining its enabling technologies and sensor systems. Additionally, it presents a six-layered architecture of IoT and highlights the associated key challenges.

C. Gupta and his team (Gupta et al., 2018) [12] explore various security threats in wireless networks and conduct an in-depth survey on the subject. These threats include access control attacks, authentication attacks, breaches of confidentiality, and others.

D. Ilyas and colleagues (Ilyas et al., 2017) [14] discuss numerous applications of wireless sensor networks in healthcare and address future research prospects related to the utilization of such networks in healthcare settings.

E. Talpur and co-authors (Talpur et al., 2021) [15] review the pivotal role of IoT in healthcare monitoring systems and its involvement in both academic research and practical applications.

F. Dziak et al. (Dziak et al., 2019) [16] propose a methodological approach for developing IoT-based information systems for healthcare applications, targeting both indoor and outdoor use. This approach is validated through a comprehensive study of real-life scenarios where support for elderly individuals, especially those with limited mobility living alone, is essential

III. Services and Application of IOT in healthcare

To monitor a patient's health condition, small medical devices are either implanted in the body or worn externally. It's worth noting that services are typically driven by developers or engineers, while applications are driven by clients, in this case, patients. To categorize various services and applications of IoT in the medical field, the following terms are defined:

A. Ambient Assisted Living (AAL): Ambient-assisted living integrates with ambient intelligence technologies and home automation to create a responsive system. An IoT platform powered by artificial intelligence that monitors the healthcare of elderly and disabled individuals is termed ambient assisted living (AAL). The goal of this service is to provide independence to seniors in their own homes in a straightforward and safer manner. For IoT-based AAL, aspects such as communication, security and privacy, control, and automation are proposed.[5].

B. Children's Health Information (CHI): Addressing issues related to emotional, behavioral, or mental health problems in children, as well as the need for proper health checks and nutrition, led to the development of the Children Health Information (CHI) service. Several CHI services are designed to educate children about proper nutrition or address other child-related issues with the help of parents, teachers, guardians, etc.

C. Tele-Health :Data from system devices is transmitted to the doctor's office. This involves collecting and processing specific patient information, enabling healthcare automation that constantly compares current records with past records to determine the future course of patient management. Tele-health allows access to healthcare resources from PCs, phones, etc., from any location. This service is highly sought after, with various applications available on the market, such as heartbeat counters, calorie burners, cardiac information, etc. Physiological parameters are sensed by smart watches, and many researchers are actively working on improving tele-health services. [6] [7].

D. Some Applications: Applications include numerous real-time health monitoring biomedical embedded systems capable of detecting ECG signals[8] [9], heart rate, body temperature [10], accelerometers, blood pressure, arterial oxygen saturation, blood glucose levels, etc. This framework system enables healthcare providers to monitor the medical condition of the subject and provide applicable services. In this classification of applications, most studies and models share similar functionalities and properties, such as data collection, capture, storage, and transmission of vital signs. Additionally, these applications face similar challenges

IV. Major Challenges in Health Monitoring System

A. Security and Privacy: Inadequate consideration of security requirements often exposes patients to privacy risks when deploying wireless technology in health monitoring systems. The transmission of information over the internet poses threats to patient data. Key security requirements include availability, integrity, confidentiality, access control, and authentication. Security concerns in health monitoring systems mirror those in conventional networks, with cryptographic methods employed to protect patient data against attacks.

B. Power Consumption: Energy consumption is a significant concern alongside data security. Health monitoring systems should utilize devices and protocols with low power consumption to conserve energy for further use. As these systems incorporate numerous biosensors and devices, considerations should be made regarding the power consumption of devices, protocols, and communication gateways. Developing a sustainable IoT infrastructure poses challenges in achieving energy efficiency.

C. Accurate and Continuous Monitoring: Patients with chronic diseases require continuous monitoring to promptly detect any abnormal activity

D. Storage Capacity: Although storage capacity in IoT technologies is increasing, there is a need to ensure efficient storage of large amounts of patient data in minimal space. Lossless compression techniques are essential for medical data due to its sensitivity

E. Standardization: The healthcare sector sees a proliferation of products and devices from various vendors, often without adherence to standard interfaces and protocols. This lack of standardization creates challenges in interoperability and data exchange. Standardization issues also extend to electronic health records, where multiple governing bodies are involved.

F. Data Transmission: Selecting the appropriate method for transferring sensor information to back-end servers for processing and analysis poses a significant challenge in health monitoring system development, particularly in wireless body area network applications. Different data transmission types, including multicast, broadcast, unicast, and anycast, each have unique considerations regarding efficiency, network traffic, and energy utilization.

G. Data Protection: Ensuring the protection of health information acquired from various sensors and devices against unauthorized access is crucial. Challenges in data protection encompass physical security, secure routing, data transparency, and managing IoT big data securely.

.

H. Data Portability: Concerns regarding the ability to switch to another cloud vendor or return to the healthcare organization without disrupting operations or encountering conflicts with data arise with cloud computing adoption. The challenge lies in transitioning to a new cloud service provider smoothly, highlighting the need for supplier considerations addressing termination rights, data access and retrieval rights, assistance with migration, and exit clauses in contracts.

V. Security Threats

Outlined below are various attacks related to access control, authentication, and availability:

A. Access Control Attack (ACA): ACA occurs within systems where professionals oversee access to specific areas and resources in a computer-based network that holds valuable data. The objective of these attacks is to breach the wireless network's security by bypassing controls such as access point MAC filters and Wi-Fi port access controls. Examples of such attacks include Rogue Access Points and MAC spoofing.. [12].

B. Authentication Attacks: Authentication attacks are employed by malicious actors to compromise a user's private identities and credentials. This unauthorized access enables them to infiltrate other private services or systems.

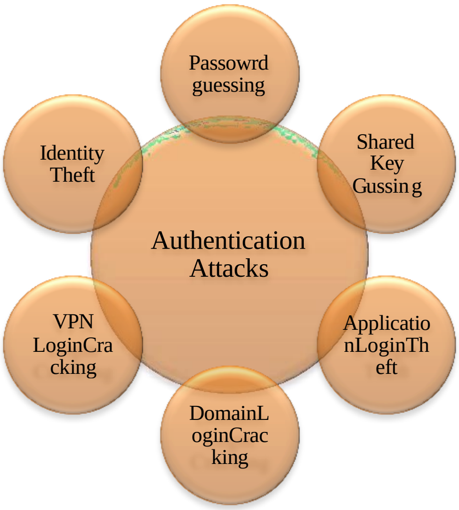

Fig.3Authentication Attacks

C. Availability Attacks: Availability attacks, particularly Denial of Service (DoS) attacks, pose a significant threat to network security. These attacks disrupt network functionality by utilizing methods like the Carrier Sense Multiple Access (CSMA) technique to create the illusion of an occupied channel. They can occur either intentionally or accidentally. Attackers often disrupt network operations by using RF signal generators to jam transmissions.

VI. Cryptography Solution for Data Protection

One of the critical aspects of an IoT- based health monitoring system is ensuring data security. Cryptography, often referred to as encryption, is fundamental in achieving this. It involves the study of mathematical techniques for securing data in various forms. Cryptography entails converting information into a code for transmission over a public network, transforming the initial text into a coded equivalent known as "cipher text" using a coding rule. This cipher text is then decrypted at the receiving end to revert to plaintext. Employing cryptography allows us to secure sensitive patient health records effectively. Cryptography is commonly categorized into two types: symmetric and asymmetric cryptography.

A. Symmetric Cryptography: Symmetric encryption utilizes a single key, known as a secret key, for both encoding and decoding electronic data. Parties communicating via symmetric encryption must share this key to facilitate the decryption process. In simpler terms, symmetric cryptography uses only one key for both encryption and decryption of data. Examples of symmetric cryptography algorithms include AES, DES, DES3, and TWOFISH.

B. Asymmetric Cryptography: Asymmetric cryptography employs two distinct keys: a public key and a private key. The public key is used by anyone wishing to send data, while only the intended recipient possessing the private key can decrypt the data. Examples of asymmetric cryptography algorithms include Diffie-Hellman, RSA, ElGamal Encryption Algorithm, ECC, and DSA. One widely used asymmetric algorithm is RSA (Rivest-Shamir-Adleman), renowned for ensuring secure communication over networks due to its lengthy key generation process. [13].

A. Algorithm for RSA: Key Generation:

1. Compute two prime numbers, p and q, where p ≠ q.
2. Calculate the modulus n, such that n = p * q.
3. Determine Euler's totient function φ, where φ = (p-1) * (q-1).
4. Select an exponent e, which is coprime with φ(n) and satisfies the condition 1 < e < φ(n).

B. Encryption and Decryption Algorithm:

1. Obtain the public key (n, e) and represent the plaintext message as a positive integer m.
2. Compute the ciphertext c = m^e (mod n).
3. Use the private key (n, d) to compute m = c^d (mod n).
4. Retrieve the plaintext from the integer representation m.

VII. Conclusion

This paper has delved into the applications and challenges of iot in healthcare. Researchers are actively striving towards the establishment of a digitalized healthcare system by leveraging existing healthcare services and medical resources.

References

[1] J. S. Kumar and D. R. Patel. 2014. “A survey on internet of things: Security and privacy issues,” *International Journal of Computer Applications*, vol. 90, no. 11.

[2] F.Andriopoulou,T. Dagiuklas, and T. Orphanoudakis. 2016. “*Integrating IoT and Fog Computing forHealthcare Service Delivery”*, Springer International Publishing.

[3] M. M. Hossain, M. Fotouhi, and R. Hasan. 2015. “Towards an analysis of security issues, challenges, and open problems in the internet of things,”, *IEEE*, (pp. 21– 28).

[4] S. Alasmari and M. Anwar, “Security & privacy challenges in IoT-based health cloud.2016.” in *Proc. International Conference on Computational Science and Computational Intelligence, IEEE*.

[5] M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara.2013.”A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN)," in *Proc. 7th Int. Conf. Innov. Mobile Internet Services.*

[6] Ganesan, R., Kanimozhi, K., Prakash, R., and Chamundeeshwari, V.Vijaya.2015. “Internet ofThings (IoT) Enabled Wireless Patient Monitoring System using CC3200,” *Australian Journal of Basic and Applied Science.*, 9(16): (pp. 275-281).

[7] Hussian, Chesti. Altaff , K. Vuha, K., Rajani, M.,and Vineeth Madhu.2017.” Smart Health Care Monitoring using Internet of Things and Android”, *International Journal of Advanced Research in Electronics and CommunicationEngineering(IJARECE),* vol.6,(pp.101-104).

[8] integration of intelligent packaging, unobtrusive bio- sensor, and intelligent medicine box”,"IEEE Trans. Ind. Informat., vol. 10, no. 4,(pp. 2180-2191).

[9] R. Ramu and Kumar Dr. Sukesh.2018.” IOT based real- time ECG monitoring of rural cardiac patients”, International Journal of Engineering &Technology,(pp. 806-809) 2.

[10] Sahu, Mohan Lal and Kaushal, Jigyasu Kumar.2017.” Real time health monitoring system using Arduino and LabVIEW with GSM Technology," International Journal ofAdvanceEngineering &ResearchDevelopment,(pp.1- 5).

[11] Farooq, M.U., Waseem, Muhammad, Mazhar, Sadia, Khairi, Anjum and Kamal, Talha.2015.” A Review on Internet of Things (IoT)”, International Journal of Computer Applications, vol. 113 - No. 1, (pp. 1-7).

[12] Gupta, Akhil and Jha, Rakesh Kumar.2015.” Security Threats of Wireless Networks: A Survey”, International Conference on Computing, Communication and Automation, pp. 389-395.

[13] Nisha, Shireenand Farik, Mohammed.2017. “RSAPublic Key Cryptography Algorithm–A Review”. International Journal Of Scientific & Technology Research, Vol. 6,(pp. 187-191).

[14] Ilyas ,Mohammad.2018.“Wireless Sensor Networks for Smart Healthcare” IEEE, (pp. 1-5).

[15] Talpur, Mir Sajjad Hussain.2013. “The Appliance

Pervasive of Internet of Things in Healthcare Systems," International Journal of Computer Science Issues, vol.10, (pp. 419–424.)

[16] Dziak, Damian, Jachimczyk, Bartosz and Kulesza, Wlodek J.2017." IoT-Based Information System for HealthcareApplication:DesignMethodologyApproach", Applied Science Journal, (pp. 1-17)