A SURVEY ON POTENTIAL SECURITY CHALLENGES IN INTERNET OF THINGS (IOT) BASED ELDERLY CARE

V. Rani, S. Hemalatha*

Abstract

The internet of things (IoT) is an intelligent connection of people, process, data, and things. The internet of medical things (IoMT), software, and mobile technological revolutions are enabling it to offer greater efficient and effective elderly care. Due to the diverse technologies and gadgets we use, the data we acquire has offered new opportunities for hostile hackers. Health Service Providers (HSPs) rely upon these gadgets to perform their operations, but for the motives stated above, they're not able to accept as true with them. They pose a major risk to enterprises and their patients because they frequently ship with vulnerabilities, run on unsupported operating systems, and are difficult to fix. This paper analyses numerous security issues and unpatched vulnerabilities.

Keywords: Cyber attackers, HSPs, IoT, IoMT, Medical devices, Elderly care, Security holes

I INTRODUCTION

The current trends in Internet-of-Things (IoT) generation can play a lead function in designing appropriate healthcare structures for the aged. Efforts, overall performance expectations, normative effects, and mitigation fame have an effect on the behavioral intentions of aged customers the use of clever houses for clinical and fitness care functions in a top-quality wonderful way. It is tedious to steady the communicated facts and for the motive of tool identity. The version recommends and substantiated through way of means of the writer is completely associated with senior humans and consists of the factor this is unique for inhabitants. The mixture of the Unified Theory of Acceptance and Use of Technology (UTAUT) conceptual framework has incorporated in to a new system being proposed for the clever houses specially designed for the aged people fitness in customer perspective [1]. Existing safety strategies are especially famous at the net are too complicated to combine on small and restrained objects. This gives a survey of current safety conventions utilized in IoT, their contrast, and realistic answers for diverse attacks.

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

II RELATED WORKS

There are several evaluated studies at the protection of IoT. A study targeted on safety worrying conditions and others targeted on safety solutions that supported one-of-a-type of scientific procedures and tools. The study [2] furnished lots of connected thing's safety worrying conditions and additionally about fog, aspect computing, block-chain, and tool reading generation due to the various ways of measuring connected things safety.

In this paper [3] the authors targeted the perception layer safety, protocols, and handover defences for mobile-IoT. The authors compared the existing security features for mobile IoT applications. A structured evaluation has a have a take observe [4] investigated hardware and software-based definitely protection functions for IoT mobile computing devices. Different authentication strategies for the IoT and defined numerous security affirmation mechanisms are featured [5]. They moreover furnished succeeding commands for research on verificationsystems. Researchers [6] assessed present-day safety solutions, factors for global positioning and location-based definite IoT and also pointed out the safety threats and vulnerabilities of internet layers of IoT [7]. It describes the present-day tool reading-based

definitely audit trial machines and explored them in terms of spotting techniques and confirmation mechanisms. They have observed and [8] inspected phishing threat based mostly on various information belongings at the side of Internet of Things stationing environments and architectures. They collated unique information assets from the type of layers, regulations on functionality exertion of data origins and strategies.

III OVERVIEW, SAFETY ARCHITECTURE, EDERLY CARE

Even with a few possibilities and applications, there are great IoT protection problems that want to be labeled. In the variety of healthcare applications the usage of IoT is developing swiftly day by day and the cause is the improvement of sensor devices. Progress in the IoT era have resulted withinside the evolution of traditional homes to smart homes which ensures a better pleasant of life for its populace through home networking. IoT eldercare can be able to generate a huge amount of records for humans and organizations, which can be prone to threats. Since the low-strength IoT devices are typically set up in antagonistic physical environment, more robust protection techniques want to be done similarly to conventional IT protection techniques.

A. Overview

IoT permits the interrelation of numerous disparate gadgets and net works the usage of specific verbal exchange technologies. Communication may also arise among machine, things, and human via a specific approach of connectivity. IoT targets to offer clever and superior offerings to its customers via facts networks shaped with the aid of using constant integration of bodily items. The items are webbed or related to the net or people and are able to transmit instantaneous facts approximately related to patients.

B. SafetyArchitecture

In IoT architecture, it's miles in general working on three layers that are the sensor, interconnected, and application layer. Every individual stage of architecture has inherent safety concerns.The succeeding figure 1 depicts the safety architecture of IoT.

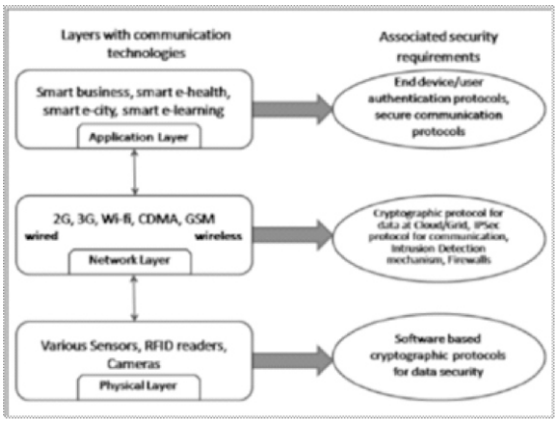

Fig.1: IoT Safety Architecture

C. IoT in Homecare for the Elders

People's bodily and mental needs extrude with age. The foremost task is to apprehend the conduct of older human beings towards a provider this is currently now no longer to be had on a business scale. Hence, there's an extreme loss of modern-day recognition is at the underlying technology and offerings in preference to an end-person perspective. In this study, the writer specializes the elements that impact the attractiveness of smart houses for healthcare conceptually in preference to a particular product or provider.

Fig.2: Conceptual view of a smart home

IV SECURITY MEASURES, ATTACKS, CHALLENGES AND COUNTERMEASURES

With the massive adoption of the IoT withinside the healthcare domain, it's miles crucial to perceive and examine the wonderful capabilities of IoT safety and privacy, which include safety requirements, vulnerabilities, chance fashions, and countermeasures, from the healthcare perspective. Following are the safety measures we took into consideration in healthcare.

A. Security Measures/goals

1) Confidentiality- It is crucial to make certain safety and availability of the record to the simplest legal users.

2) Integrity- It makes positive that obtained clinical records are not altered in transit through an adversary.

3) Availability- It guarantees the survivability of IoT healthcare offerings (both neighborhood or international or cloud offerings) to accredited events while wanted even under denial-of-carrier attacks.

4) Authentication- It permits an IoT fitness tool to make certain the identification of the peer with which its miles communicating.

5) Authorization- It guarantees that simplest accredited nodes are available for community offerings or resources.

6) Fault Tolerance- It is a safety scheme that has to hold presenting respective safety offerings even withinside the presence of any fault.

7) Lightweight Solutions- It is completely a unique safety function primarily based totally on encryption or authentication of statistics and gadgets in IoT.

8) Heterogeneity- The IoT connects extraordinary entities with extraordinary capabilities, complexity, and vendors. Therefore, protocols should be designed for paintings in plenty of gadgets in addition to in the extraordinary situations. The IoT objectives at connecting tool-to-tool, human-to-tool, and human-to-human, accordingly it offers a connection among heterogeneous matters and networks. And to make sure safety, a top-quality secret writing device is required with good enough key control and safety protocols.

9) Key ControlMechanism- The connected instruments and sensors want to change a few encryption substances it must make sure the confidentiality. For this, there should be a need of lightweight key control mechanism for all frameworks which can allow accepting as true among various things and might distribute keys through ingesting gadgets' minimal capabilities [9].

B. Security Attacks

Security assaults may also cause hundreds or thousands of bucks in losses to big agencies and highbrow assets theft. Figure 3 depicts the taxonomy of feasible safety assaults layer-wise.

Fig.3: Layer-based IoT Security Attack Taxonomy

The authors analyzed the safety assaults primarily based totally on IoT property and their properties. They are tool property, region property, assault level, assault strategy, harm

level, host-primarily based totally assaults, and protocol assaults [10].

D. Challenges and Limitations

Threats and protection issues in IoT-primarily are based totally on programs like healthcare structures are proven in Table 1.

Layer	Security Concerns and Threats
Perception	Wireless signal strengths, physical attacks, dynamic IoT topology
Network	Traffic analysis, eavesdropping, passive monitoring, heterogeneity of network components and protocols
Application	Absence of global and standard trust policies, authentication mechanisms

Table 1: The security concerns and threats in IoT-based applications

A mission that still remains is their acceptance (ease-of-use of every hardware and software program application software program application person interfaces, comfort, size, weight, and battery lifestyles/electricity consumption settings). Most useful balance amongst the ones comfort parameters, typically positioned within side the retail way of lifestyles software application program with a few different impediments are the shortage of interoperability and no longer usage platform. Finally, security, confidentiality, and ethics are residual concerns. Although there are big consistent storage and authentication techniques, the enterprise wishes to benefit from IoT-particular frameworks for extra e_client or self-enough authentications of devices [11].

V COUNTERMEASURES FOR SECURITY ATTACKS IN IoT

Each IoT layer is created from a hard and fast of protection protocols, techniques, algorithms, and protection kits hired to make it tougher for an adversary to strike or hack into the system. Higher expertise of those conceptions will permit the researchers to examine the safety breaches and the extent of protection this is needed. With this, encroachment detection, prevention systems, and different whole protection answers may be implemented to defend IoT from the protection threats. The authors introduced collectively the prevailing counter measures which include learning-primarily based totally, encryption-primarily based totally, autonomic, and different strategies to stable IoT structures from the application, community, and bodily layers.

1) Learning-based counter measure - based primarily on ML / DL to detect intrusions.

2) Autonomic Approaches - self-stable / autonomic Approaches that are able to figure out and shield themselves from random assaults with MAPE architecture.

3) Encryption-Based Countermeasures – symmetric and uneven cryptographic countermeasures for securing IoT [10].

VI CONCLUSION

According to the study, we've got consolidated and offered about the possible technologies, types of threats, and compared the elements associated with imposing a complete protection method in IoT with conventional internet. IoT framework from one organization to a collection of various groups and distinctive structures, numerous protections want to be addressed. The IoT has an extremely good ability to convert the manner we stay today. But, the most important necessity is in awareness of clever framework is protection. If protection worries like privacy, confidentiality, authentication, get entry to control, stop-to-stop protection, consider management, worldwide rules and requirements are conveyed absolutely, then a change of the whole lot through IoT may be estimated in the future.

REFERENCES

[1] Debajyoti Pal, SureeFunilkul, NiponCharoenkitkarn, "Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective",doi:10.1109/Access.2018.2808472.

[2] V.Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, andsolution architectures",IEEE Access, vol. 7, pp. 82721_82743, 2019,doi: 10.1109/Access.2019.2924045.

[3] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, andJ. Lim, "Security, privacy and trust for smart mobile- Internet of Things(M-IoT): A survey", IEEE Access, vol. 8, pp. 167123_167163, 2019,doi: 10.1109/Access.2020.3022661.

[4] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysisof IoT devices by using mobile computing: A systematic literaturereview", IEEE Access, vol. 8, pp. 120331_120350, 2020,doi: 10.1109/Access.2020. 3006358.

[5] T. Nandy, M. Y. I. B. Idris, R. Md Noor, L. Mat Kiah, L. S.Lun, N. B. AnnuarJuma'at, I. Ahmedy, N. Abdul Ghani, and S.Bhattacharyya, "Review on security of Internet of Things authenticationmechanism", IEEE Access, vol. 7, pp. 151054_151089, 2019, doi: 10.1109/ACCESS.2019. 2947723.

[6] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko,H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara,S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, andH. Kuusniemi, "Robustness, security and privacy in location-basedservices for future IoT: A survey", IEEE Access, vol. 5, pp. 8956_8977,2017, doi: 10.1109/Access.2017.2695525.

[7] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques", IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2671_2701,3rd Quart., 2019, doi: 10.1109/COMST.2019.2896380.

[8] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detectionapproaches with IoT perspective," IEEE Access, vol. 8, pp. 78847_78867,2020, doi: 10.1109/Access.2020.2990195.

[9] Goutam Kumar Saha and Sandeep Kumar, "Security Issues in IoT-Based Healthcare", doi: 10.5958/0975-8089.2017.00036.7.

[10] Shapla Khanam, Ismail Bin Ahmedy, Mohd Yamani Idna Idris, "A Survey of Security Challenges, AttacksTaxonomy and Advanced Countermeasuresin the Internet of Things", date of publication November 11, 2020.

[11]Thanos G. Stavropoulos, AsteriosPapastergiou, LamprosMpaltadoros, Spiros Nikolopoulos, and IoannisKompatsiaris, "IoT Wearable Sensors and Devices in Elderly Care:A Literature Review", Published: 16 May 2020.