IoT Sensors for Smart Health Devices and Data security in Healthcare

Lu Jiang
School of Communication and Design, Sun Yat-sen University, Guangzhou, Haizhu District, China.
luluji220@hotmail.com

Article Info
Journal of Biomedical and Sustainable Healthcare Applications (http://anapub.co.ke/journals/jbsha/jbsha.html)
Doi: https://doi.org/10.53759/0088/JBSHA202101013
Received 18 October 2020; Revised form 30 December 2020; Accepted 25 April 2021.
Available online 05 July 2021.

Abstract – Smart applications and monitoring systems across health systems are provided by the Internet of Things (IoTs), which connects devices and networks, and potentially deliver new technologies in this field. In order to establish an IoT-based healthcare system that protects patients' sensitive and personal information, it is imperative that security be ensured. It was our goal to identify the elements and ideas connected with the security needs of the Internet of Things in the healthcare sector. In the healthcare industry, a survey was done on the security needs of IoTs devices. Data from Web of Science, IEEE, Scopus, and PubMed has been searched since 2005. In addition, we adhered to international norms and recognized rules for cyberspace security. This paper presents an an analysis of the aspects and ideas relevant to the security needs of IoTs in a medical environment. Our research revealed two major categories of security needs: cyber resilience and cyber security. In the cyber security category, there are CIA (Confidentiality, Integrity and Availability) Triad and the non-CIA subcategories. Information security (Confidentiality, Integrity and Availability represented the CIA triad), performability, survivability, maintainability, safety, and reliability were listed as the primary elements for cyber resilience needs. The trustworthiness of Healthcare Internet of Things (HIoTs) relies on balancing traditional (cyber security) and unique (cyber resilience) needs.

Keywords – Internet of Things (IoTs), Healthcare Internet of Things (HIoTs), Electrocardiogram (ECG), Confidentiality, Integrity and Availability (CIA)

I. INTRODUCTION

The phrase " Internet of Things" (IoTs) was invented by Kevin Ashton in 1999 as an innovative concept [1]. Using this method, many gadgets and objects can communicate without the need for human intervention. To understand the Internet of Things, one must first understand how it relates to reality and the natural world. The IoTs may assist with transportation, farming, intelligent cities, emergency services, and logistics, just to name a few. In addition, the medical business is one of the most promising industries for IoTs deployments. For example, IoT-based healthcare solutions include monitoring patients remotely, smart wellness, and assisted living. For patients who need constant monitoring and preventive treatment, IoTs and medical devices work together to enhance medical services and deliver a real-time status report. IoTs helps to diagnose and treat diseases early in areas such as exercise, chronic sickness, and geriatric care by assisting in the diagnosis and treatment process.

A wide range of health issues have been addressed via services and ideas that have had a significant impact on the industry. More and more services are being offered on a daily basis as a result of expanding healthcare demands and new technology breakthroughs. Healthcare Internet of Things (HIoTs) system architectures [2] increasingly include these elements as a requirement. Each healthcare provider in an HIoTs setting offers a variety of therapeutic services. There isn't a single definition for any of these ideas or services. HIoTs systems are distinguished by their implementations. Resultantly, it is impossible to define each concept in broad words. The next part, however, outlines a few of the most often used IoTs health services in order to set the scene (see Fig. 1).

While IoTs has many advantages, it also brings with it an increased risk of security breaches and vulnerabilities in medical systems. It's for these reasons why this has happened: Patients' vital information is the primary goal of clinical instruments, which are used to acquire and communicate data; the IoTs phenomena produces inconsistencies and complexities; and medical IoTs device producers disregard security considerations. The aforementioned considerations have led to an increase in the number of people worried about the Confidentiality, Integrity, and Accessibility (CIA) of information.

Examples of IoTs applications in medical include programs and equipment that monitor and manage an individual's vital signs. Although these techniques may be exposed to security issues e.g., privacy, authorization and verification threats. Cybersecurity has become a big issue in the medical business. Device weaknesses might be used by hackers to compromise the IoTs framework. When it comes to resolving attacks, standard security standards are irrelevant because of the limitations of medical technology.

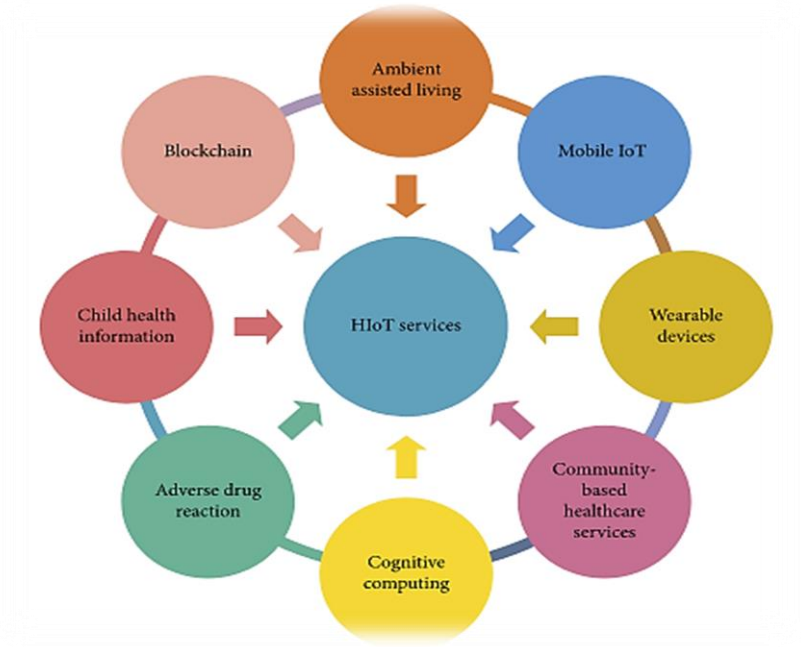

Fig 1. Widely used HIoTs services

So, in terms of security and privacy, healthcare IoTs technologies must be considered. To prevent medical information from leaking, the Health Insurance Portability and Accountability Act (HIPAA) has implemented technical and physical protections. There has to be a more robust approach to implementing these measures, since they were inadequate [3]. Resultantly, defining the security demands of a secure IoT-based healthcare infrastructure is essential. To achieve the rationale of this research, this paper has been organized as follows: Section II presents a review of the relevant literature texts. Section III presents an overview of research objectives. Section IV focuses on the methodology of the research. Section V presents results of the analysis while Section VI presents an analysis of the discussion. Section VII concludes the research.

II. LITERATURE REVIEW

Tariq et al. [4] posits that the IoTs paradigm for healthcare systems makes it easier to combine the benefits of IoTs innovation and cloud technology with the area of healthcare. It also specifies the procedures for transferring patient information from a variety of monitors and medical equipment to a specific healthcare system. The organisation of diverse elements of an IoTs medical mechanism that are consistently integrated in a healthcare context is referred to as the topology of an HIoTs. The author, broker, and subscribers are the three major elements of a basic HIoTs network. The publisher symbolises a network of linked detectors and other health equipment that may capture the person's vital data independently or concurrently. Hypertension, heart rate, temp, oxygen levels, ECG, EEG, and EMG are just a few of the variables that may be measured. This data may be regularly sent to a broker by the publisher over a system. The broker is in charge of cloud data storage and processing. Lastly, the subscriber engages in constant surveillance of the person 's data through a smartphone, pc, tablet, or other device.

As per Yan et al. [5], the electric function of the heart is represented by an Electrocardiogram (ECG), which shows the hyperpolarization and repolarization of the atrial and ventricular. An ECG is a kind of electrocardiogram that shows the fundamental impulses of the cardiac muscle and may be used to detect different cardiac problems. Arrhythmia, extended QT intervals, myocardial ischemia, and other anomalies are among them. The use of IoTs innovation in the early diagnosis of cardiac problems via ECG surveillance has shown promise. In the past, IoTs has been used in ECG monitoring in a number of research projects. A portable data gathering system and an accepting processor are presented by Puneeth and Ganesha Prasad [6], which is an IoT-based ECG surveillance system. It made use of a real-time search automated technology to identify cardiac abnormalities. A compact portable low-power ECG monitoring device incorporated with a t-shirt was presented Gupta et al. [7]. It collected high-quality ECG data using a biopotential chip.

The captured information was then sent to the end users through Bluetooth. A smartphone app might be used to see the captured ECG data. The suggested technology may run on only 5.2 milliwatts of electricity. After combining an IoTs system with big dataset analysis to handle increased data collection, real-time surveillance in an IoTs network may be conceivable. By combining the concepts of nanoelectronics, cloud computing, and IoTs, many scholars have presented a surveillance framework for ECG, which potentially manages constant and long-term surveillance. Romagnoli et al. of [8] attempted to overcome the problem of energy usage in a portable ECG surveillance device. They have presented compressive detection, a novel approach for reducing power usage and improving ECG monitoring effectiveness. Al-Kababji et al. [9] describes an IoT-centred fall surveillance and ECG surveillance framework, which potentially employs the cloud-centred mobile and

computer application. This device was created to offer older patients' real-time supervision by constantly examining their ECG and sensor data.

Li et al. [10] utilized ECG information to analyse the information and provide feedback if any physiologic anomalies or deterioration in the patient's condition is detected. The HIoTs combines separate elements into a mixed grid in which each element on the IoTs system and internet in the health system serves a specialised role. It's difficult to offer a common framework for HIoTs since the topology relies on the medical need and implementation. For an HIoTs system, several fundamental modifications have been implemented in the prior. While implementing a new IoT-based medical system for real-time client surveillance, it's critical to make a list of all relevant actions associated with the desirable health applications. The IoTs system's success is determined by how well it meets the needs of healthcare practitioners. Because each ailment necessitates a complicated set of healthcare actions, the topology must adhere to medical regulations and procedures throughout the diagnostic process.

Savitha [11] posit that the techniques that are employed to create an HIoTs network are very important. It is because the usage of certain technologies may improve an IoTs program's capability. As a result, a variety of cutting-edge techniques have been used to link diverse medical implementations with an IoTs systems. These techniques could be grouped into three categories: identity, communications, and positioning. An important aspect in creating an HIoTs network is the availability of patients' data from the nodes that have been approved (sensors), which could be located in faraway places. These sensors and nodes in the health system may be identified effectively to achieve this goal The procedure of issuing a unique identifier (UID) to each authorised organisation is the first step in establishing identification and enabling clear data transmission. Every healthcare resource (hospital, doctor, nurse, caretakers, medical equipment, and so on) has a unique identifier (UID) attached to it. This guarantees that resources can be identified and connected in a digital environment.

Grover [12] posit that one may find several guidelines in the literature on how to identify anything. Both a GDUID (Globally Developed Unique Identifier) and a UUID (Universally Unique Identifier) have been established by the Open Software Foundation (OSF) (GUID). Centralised coordination is not required to run the Distributed Computing Environment's UUID. The detectors and controllers in a health system are recognized and handled independently, which aids in the system's correct working. It is possible, nevertheless, that as IoT-based technologies evolve, their ability to uniquely identify individual components may shift over time. So, the gadget must offer an option to upgrade this information in order to keep its integrity intact. A possible explanation for this is that the configuration change not only impacts the tracking of network components, but it may also result in an incorrect diagnosis. As a result, IoTs in healthcare requires new technologies capable of (1) locating things using a worldwide identification code, (2) effectively monitoring the identities of the elements using several encryption and authentication approaches, and (3) establishing global directories evaluating the critical analysis and discovery of IoT systems based on UUID.

As per Ahmed, Jeon, and Piccialli [13], several entities may communicate with one other using various communication methods, in an HIoTs system. There are two types of communication technology in this category: short-range and medium-range. When it comes to short-range and wide-range communication protocols, the former are the ones that are employed in the connection components within a particular range or BAN (Body Area Network), whereas the medium-range protocols are those that may be used to communicate over a longer distance. Short-range communication may range from a few centimetres to a few metres in distance. In the vast majority of IoTs scenarios, short-range connectivity is recommended. RFID, Wi-Fi, Zigbee, and Bluetooth are just a few of the more popular methods of wireless communication.

Radio-Frequency Identification (RFID).

A Radio-Frequency Identification (RFID) tag may be used to communicate across short distances (10 cm–200 m). Tag and reader are the two components. The tag is built with a microprocessor and antennae. Devices in the IoTs context may be identified by a unique identifier [14]. Radio waves are used by the reader to communicate with a tag attached to the item and exchange data. In the case of IoTs, the tag contains an Electronic Product Code (EPC). Using RFID, healthcare practitioners can detect and monitor medical equipment more quickly and effectively. For the most part, RFID does not require an exterior power supply. In spite of this, it is considered an unsafe protocol and could have compatibility problems whenever employed in mobile devices.

Bluetooth.

The short-range wireless communications via UHF (Ultra-High Frequency) [15] waves are another feature of Bluetooth. Medical gadgets may communicate wirelessly with each other using this technology. Bluetooth operates in the 2.4 GHz band. Communication range is up to 100 metres using the Bluetooth protocol. Data is protected via Bluetooth using authentication and encryption mechanisms. Bluetooth's cheap cost and power efficiency make it a good choice for many applications. It also helps to reduce data transmission interference between the devices that are linked. The problem arises when long-range communication is needed for healthcare applications.

Zigbee.

A common protocol for transmitting information between medical devices is Zigbee [16]. Comparable to Bluetooth's (2.4 GHz) frequency band, Zigbee has a similar range. Even so, it has a greater connection range than Bluetooth-enabled gadgets. Network topology is based on the mesh network model. Routers and a central processing unit make up the network infrastructure Data gathering and analysis are handled by the processing centre. Even if one or two sensors fail, the mesh

network maintains a constant link between them all. Zigbee's low energy usage, larger network capacity, prompt rate of transmission make it a good choice.

Near-Field Communication (NFC).

Near-Field Communication (NFC) [17] is based on electromagnetic induction between two antennas positioned close to each other. Similar to RFID, this technique employs electromagnetic induction to transmit data. Both active and passive modes are available for NFC devices. While transmitting radiofrequency waves, only one device creates them, which means that only one device receives them while in passive mode. As long as the radio frequency is on, the two devices may communicate with each other without pairing. An easy-to-use interface and a reliable wireless network are two of NFC's most appealing features. But it only works over a small distance of time.

Wi-Fi

Wi-Fi, a Wireless Local Area Network (WLAN) [18], follows the IEEE 802.11 protocols. This technology has a greater communication range than Bluetooth (about 70 ft.) Wi-Fi networks may be established fast and simply. As a result, hospitals are where you're most likely to find it. Due to its ease of use with smartphones and ability to enable rigorous security, Wi-Fi is widely used. But it consumes a lot more power, and the network is unreliable.

Satellite.

Distant, mountainous, or oceanic locales that are difficult to reach by conventional means of communication rely on satellite communication because it is more reliable and efficient than other options. Received signals from Earth are amplified and sent back to Earth by the satellite. More than two thousand satellites revolve the globe. On of the merits of satellite communications is the capacity to send large amounts of data quickly, as well as the reliability and compatibility that come with it. Satellite communication, on the other hand, consumes a lot of energy compared to other methods of communication.

Healthcare networks employ RTLS (Real-Time Location Systems) [19] or area initiatives to survey and identify potions of a particular items. Tracking the treatment methods depending on the allocation of resources is also a feature of this software. In terms of technology, the Worldwide Position System, more often known as GPS, is among the most frequently utilised systems. A satellite-based tracking system is used. As long as there is and 4 satellites and a clear field of view of items, GPS can identify it. Ambulances, doctors, carers and patients may all be tracked with HIoTs technology. As a result, the use of GPS in indoor applications is restricted since the surrounding infrastructures might function as a barrier to communication.

A Local Positioning System (LPS) may be employed in these situations. It is possible for LPS to track an item using an array of pre-deployed monitors that sense the radio signal generated by the travelling object. LPS may also be implemented via RFID, Wi-Fi, Zigbee, and other short-distance communication technologies. Due to its superior temporal precision, Ultra-Wideband (UWB) audio is favoured over conventional radios. An exact arrival time may be determined this way. An UWB-based tracking system that leverages the TDOA (Time Difference Of Arrival) has been developed by Khyzhniak and Malanowski [20]. UWB-based localization systems have also been claimed to use additional characteristics, such as the round-trip time of flight, the relative time of arrival and so on. Future smart healthcare networks may use GPS and other high-bandwidth communication technologies.

III. RESEARCH OBJECTIVE

There are a lot of sensitive and sometimes humiliating health records involved in health research, thus it is critical to protect the data that is collected and used in this research process. Security breaches may cause a wide range of consequences to anyone whose health data was improperly accessed. Personal data may create damage just because others have access to it. Economic damage might also be a problem. A person's work, medical insurance, or housing might be jeopardized if the improper information is made public. Individuals may potentially suffer social or psychological damage as a result of their participation. Infected individuals with HIV or another STD might suffer from social isolation and/or psychological trauma as a result of their revelation. Individuals may also be at risk of identity theft as a result of security breaches. It was the goal of this study to offer an analysis of the aspects and ideas relevant to the security needs of IoTs in a medical environment.

IV. METHODOLOGY

It was conducted as a literature review of IoTs security needs in the healthcare sector. Web of Scientific, Scopus, PubMed, and IEEE were among the four main digital databases that we searched. On top of all that, we went through a manual search of recognized organisations that have published security requirements for cyberspace, such as ISO, IEC, and IEEE 24765, NIST 800-160, as well as other well-known security models and reports, to find the most up-to-date information on these organisations' security requirements. In addition, the search terms included: "internet of things," "internet of things"; "ambient intelligence"; "pervasive computing"; and "heterogeneous sensor"; as well as, "machine to machine communication"; "cyber physical system"; "machine-to-machine security"; and, "smart health"; and "smart hospital"; e-health and ehealth. Study criteria were established based on the research purpose (Table 1).

Table 1. Inclusion and exclusion criteria for selection studies

I/E	Criteria	Details
Inclusion	Type of language	English-language studies
	Year of publication	Up to date research (2005 to the present)
	Location of publication	Online searches in electronic database: Research presented at conferences and in peer-reviewed publications Manual search accordance with international rules and regulations
	The scope of the research	Healthcare security and Internet of Things (IoTs) studies
Exclusion	In the absence of full-text,	Not all of the research is available online.
	Source of unrelated information	A book, commentary, editorial letter, brief message, and poster are examples of the study's many forms of publication.
	Incorrect or unrelated categorization	There is a lack of clarity in the study's content and definition of security needs.

V. RESULTS

According to Tables 2 and 3, the most important aspects of IoT security in healthcare have been uncovered and presented in this research study. IoT's security demands are classified into two categories: cyber security and cyber resilience, as shown in Fig. 2. Additional information on IoT cyber resilience and cyber security requirements could be found in the following diagrams.

Table 2. Requirements of cyber security for HIoT

	Features	Description
CIA	Confidentiality	Confidentiality guarantees that medical information is not disclosed by unauthorized parties (devices and users).
	Integrity	Integrity refers to the completeness and correctness of data throughout a system's lifespan. Integrity guarantees that an opponent does not change, erase, or distort a patient's medical data, resulting in a misdiagnosis or incorrect prescription.
	Availability	Availability guarantees that authorized users have access to medical data and equipment when they are required. It entails the availability of security services as well as the avoidance of malfunctioning and operational outages. Particularly throughout the therapy process, when clinicians should have access to timely patient data.
	Identification and authentication	Before allowing users to engage with the IoTs system's resources, identification ensures that all entities (patients, physicians, devices, and so on) are who they say they are. The process of verifying a person's or device's identification before utilizing system resources is known as authentication. Authentication of devices and apps can show that the interacting system isn't a threat and that data transferred via networks is permitted.
	Authorization (access control)	Access privileges or rights to resources must be assigned to users once their identification has been verified, so that they only have access to resources they need to do their jobs. A doctor, for example, should have greater access to a patient's medical record than other healthcare professionals.
Non-CIA	Privacy	Patients' secrets and personal information should not be shared unless they provide their permission. To provide consumers full control over their personal data, IoTs systems should adhere to strict privacy standards.
	Accountability	When anything goes wrong with an IoTs health system, the person or entity in charge of the system has to be held accountable and liable for their actions.
	Non-repudiation	It's impossible for someone to refute what they've already done. Because of this, users can verify or disprove the existence of an event.
	Auditing	All of a system's operations can be tracked and monitored in real-time by a system's ability to keep track of them. An IoTs healthcare system requires that users' actions be recorded sequentially, such as the time it takes for a user to log in.
	Data Freshness	No outdated messages should be rebroadcast because of data freshness. There are a variety of reasons why a doctor would need to know about an individual patient's Electrocardiography (ECG).

Table 3. Cyber resiliency requirements for IoT-based healthcare

Requirements cyber resiliency		
	Features	Description
Maintainability	Reliability	When devices are detecting, collecting, and sending data in potentially hazardous environments, the IoTs relies on their dependability to keep the network running smoothly (e.g., the wind, the rain, the dust, the heat, etc). As a result, dependability is defined as the capacity of a service to continue even in the face of network heterogeneity and system failures.
	Modifiability	Modifiability refers to an IoTs system's ability to be upgraded and expanded, either by adding new capabilities or making changes to those already present, at any point in its development and deployment.
	Reparability	If the system can be repaired, it means that it can be brought back to a working condition by identifying and correcting errors in the code.
	Configurability	The system's configurability happens when the settings for a set of processes may be adjusted so that the system can perform successfully in a variety of operational scenarios.
	Adaptability	When building and executing a system, adaptability/flexibility implies that the system can swiftly change and operate correctly under varied operating conditions.
	Autonomy (autonomic computing) Self-healing	IoTs systems are self-aware and able to respond appropriately to changing operational circumstances. It is characterized as a self-managing system because it protects itself, configures itself, self-heals, and self-optimizes without the need for human interaction. The following are more specific definitions of autonomy: The term "self-healing" alludes to the capability of systems to recognize and detect the breakdown of medical equipment. The system may also automatically repair and restore software and hardware components without affecting any data. Self-optimizing alludes to the capability of systems to enhance its own performance and increase service quality, as well as| optimize the consumption of resources, energy and throughput. Self-protection refers to the capacity of the system to defend from any malicious threats and attacks, and to provide alerts concerning odd events and failures. A system may be self-configuring such that faults in it can be eliminated, and the system can be restored to a defined operational condition in compliance with security policy.
	Safety	An IoTs environment's overall security may be improved by addressing concerns about the safety of devices and nodes. This attribute makes sure that the system will not encounter failure in case it experiences any catastrophic damages within a particular timeframe.
	Survivability	Survivability refers those systems continues to project IoTs networks and complete its tasks in time even though nodes and devices are hijacked and datasets are purposefully discarded. As a subset of survivability, fault tolerance is the capacity of machines or systems to operate in the events of natural disasters, and threats to their integrity.
	Performability	A performance measures (e.g., storage, accuracy, or velocity) of components or systems, which accomplishes projected functions within detailed limits is known as performability. Performance qualities of any system may be expressed as a fuzzy number that covers a range of standard levels. Therefore, measures like accuracy, precision, and timeliness may be used to assess and evaluate the performance of a system. There are a number of metrics that may be used to quantify the time it takes to execute a system job, particularly in real-time systems.

Cyber Security Requirements

A collection of conventional security criteria for patients, data, and security mechanisms is provided by the CIA Triad and non-CIA Triad components of the cyber security requirements (see Fig. 2). Users can secure HIoT from known risks and assaults thanks to cyber security, which is available to everybody. It is shown in Table 2 that confidence, stability, and

accessibility are all necessary to protect IoTs data security. Authentication, authorisation, privacy, accountability, auditing, and non-repudiation are only some of the elements of non-CIA requirements in cyber security. Table 2 summarises the elements and concepts relevant to cyber security needs.

Cyber Resiliency Requirements

In order to protect HIoT against unknown, unforeseen, uncertain, and unanticipated attacks, cyber resilience (system resiliency) has been handled as a supplementary necessity. Cyber resilient systems, as described by Yuan, Xia, and Yang [21], have the capacity to withstand and recover from inadvertent and purposeful assaults, and naturally occurring events. The resilience of systems should assure that a security approach safeguards networks, devices or data from any potential damages or attacks. There are six key types of cyber resilience qualities, as shown in Table 3, which include dependability and maintainability, as well as survivability, performance and information security. There are three dimensions of cyber resilience that overlap: accessibility, integrity and confidentiality (the "CIA trinity"). Resiliency to cyberattacks is shown in Table 3 (see above).

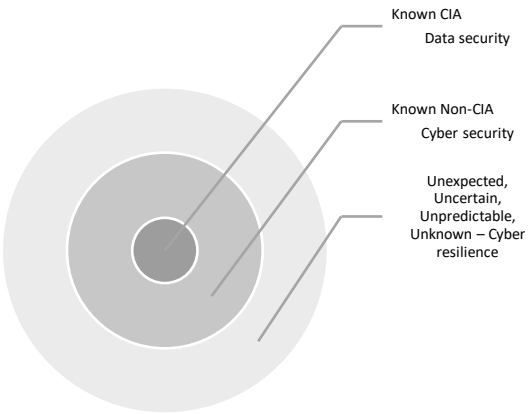

Fig 2. Security requirements in cyber space (13)

VI. DISCUSSION

We must stress that current cyber security standards only address the protection and prevention of health IoTs systems, and they do not address the vast majority of vulnerabilities and assaults. Medical sensors and devices connected to the Internet of Things (IoT) are less effective at combating recognized risks because they operate in an uncontrolled and open environment with unknown entities. This makes security and risk management in the healthcare sector more difficult than in other sectors. For example, health care providers must have prompt access to very sensitive and private patient data. Security for IoTs systems is developing from a cyber security strategy to a cyber resilience one that combines preventative, forecasting and fault tolerance features as well as autonomous computing to cover all known and unknown threats. IoTs-enabled healthcare requires comprehensive security measures, as a result. Another trustworthiness criterion is a cyber resilient system, which includes security, reliability, privacy, and safety as well as other aspects.

Customers will have more faith in medical services, which will lead to a wider use of IoTs technology if IoTs systems are able to meet both the criteria of cyber resilience and computer security. Six important cyber security requirements for IoT-based healthcare have been identified by Frikha [22] in this respect. These are: trust, identity, integrity, authorisation, accessibility, and non-repudiation. Integrity and availability are two further requirements for IoTs security, according to experts. There are several levels in an e-health IoTs architecture that need to be protected, including as verification and authorisation as well as trust management. Trust between IoTs nodes is essential, according to them, for identifying rogue devices in the network. Medical IoTs devices have been scrutinized for their security and resilience, as well as their dependability. In a trust model presented by the researchers, all layers of medical IoTs systems are incorporated, integrating communication connections, users, hardware/platform, and software. Secrecy and privacy; access control, trust management; and authentication are some IoTs security concerns. All tiers of a healthcare IoTs system should be guaranteed to fulfil trustworthy criteria, according to the researchers. Trustworthiness is achieved by adhering to all established security requirements, according to the researchers. The term "trustworthiness" refers to a system's capacity to be relied upon in all of its many aspects, including security, privacy, upkeep, performance, endurance, and so on.

VII. CONCLUSION

An Internet of Things (IoTs) system must be able to repair, adapt, and configure itself in a range of operational conditions in order to fulfil the requirements of cyber resilience. The security implications of system maintainability have been studied by many researchers in a variety of studies. A subset of maintainability, cognitive technologies are also necessary for cyber resilience. IoT-based health networks may benefit greatly from autonomic computing's ability to keep track of their own

activities. Enabling the systems to defend, configure, heal, and optimize themselves accomplishes this. Studies on IoTs security in healthcare have not addressed safety problems, which is surprising considering that safety standards play a fundamental role in the various aspects of IoTs systems, integrating medical and sensors tools. Protection measures are in place to ensure that no one is killed or injured, and no equipment malfunctions or is lost. Many IoTs applications and devices have recently been developed within the clinical setting. It is probable that intruders may target devices since they potentially handle confidential and sensitive data, e.g., personal clinical data. Healthcare Internet of Things (HIoTs) security needs need to be defined and understood. Security needs for IoT-based healthcare were explored in this research. Due to this research, scientists, information technology engineers, healthcare practitioners, and policymakers concerned about IoTs and medical technology are likely to benefit from the findings. HIoT might benefit from more research and development, as shown by this study.

References

[1]. B. Ouyang et al., "Initial development of the hybrid aerial underwater robotic system (HAUCS): Internet of things (IoT) for aquaculture farms," IEEE Internet Things J., vol. 8, no. 18, pp. 14013–14027, 2021.

[2]. M. Raza et al., "Challenges and limitations of internet of things enabled healthcare in COVID-19," IEEE Internet Things M., vol. 4, no. 3, pp. 60–65, 2021.

[3]. J. M. Kiel, "An analysis of the management and leadership roles of nurses relative to the health insurance portability and accountability act," Health Care Manag. (Frederick), vol. 34, no. 1, pp. 75–80, 2015.

[4]. F. Tariq, M. Anwar, A. R. Janjua, M. H. Khan, A. U. Khan, and N. Javaid, "Blockchain in WSNs, VANets, IoTs and Healthcare: A Survey," in Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2020, pp. 267–279.

[5]. R. T. Yan et al., "Differences between local hospital and core laboratory interpretation of the admission electrocardiogram in patients with acute coronary syndromes and their relation to outcome," Am. J. Cardiol., vol. 100, no. 2, pp. 169–174, 2007.

[6]. H. V. Puneeth and M. S. Ganesha Prasad, "Sustainable in-situ recycling and IoT-based monitoring system of water-soluble metal working fluids," Sustain. Water Resour. Manag., vol. 8, no. 1, 2022.

[7]. A. Gupta, V. Gupta, M. Mittal, and V. Mittal, "An efficient AR modelling-based electrocardiogram signal analysis for health informatics," Int. J. Med. Eng. Inform., vol. 14, no. 1, p. 74, 2022.

[8]. S. Romagnoli, I. Marcantoni, K. Campanella, A. Sbrollini, M. Morettini, and L. Burattini, "Ensemble empirical mode decomposition for efficient R-peak detection in electrocardiograms acquired by portable sensors during sport activity," in 2021 IEEE International Symposium on Medical Measurements and Applications (MeMeA), 2021.

[9]. A. Al-Kababji, A. Amira, F. Bensaali, A. Jarouf, L. Shidqi, and H. Djelouat, "An IoT-based framework for remote fall monitoring," Biomed. Signal Process. Control, vol. 67, no. 102532, p. 102532, 2021.

[10]. X. Li et al., "Roll-to-roll graphene films for non-disposable electrocardiogram electrodes," J. Phys. D Appl. Phys., vol. 54, no. 36, p. 364003, 2021.

[11]. Savitha, "A unique secure multimodal biometrics-based user authenticated key exchange protocol for generic HIoT networks," Int. j. emerg. trends eng. res., vol. 8, no. 5, pp. 1610–1619, 2020.

[12]. W. H. Grover, "CandyCodes: Simple universally unique edible identifiers for confirming the authenticity of pharmaceuticals," bioRxiv, 2021.

[13]. I. Ahmed, G. Jeon, and F. Piccialli, "A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of internet of things," IEEE Internet Things J., vol. 8, no. 13, pp. 10318–10326, 2021.

[14]. J. W. Wallace, L. C. Diamantides, K. C. Ki, and M. W. Butler, "Switched-antenna low-frequency (LF) radio-frequency identification (RFID) for ornithology," IEEE j. radio freq. identif., vol. 4, no. 2, pp. 137–145, 2020.

[15]. Q. Guan, B. Xi, and C. Zhang, "Analysis of partial discharge spectrum based on ultra-high frequency detection method," J. Phys. Conf. Ser., vol. 2030, no. 1, p. 012096, 2021.

[16]. J. K. Park, "Smart fire detector utilizing IoT-based ZigBee sensor," Indones. j. electr. eng. comput. sci., vol. 21, no. 2, p. 1132, 2022.

[17]. C. Degen, "Inductive coupling for wireless power transfer and near-field communication," EURASIP J. Wirel. Commun. Netw., vol. 2021, no. 1, 2021.

[18]. S. L. Suntu, N. H. Odongo, S. M. Chege, and O. K. Bishoge, "Robust secured roaming in wireless local area networks," Int. j. wirel. netw. broadband technol., vol. 6, no. 2, pp. 26–42, 2017.

[19]. L. Pendrill et al., "Reducing search times and entropy in hospital emergency departments with real-time location systems," IISE Trans. Healthc. Syst. Eng., pp. 1–11, 2021.

[20]. M. Khyzhniak and M. Malanowski, "Localization of an acoustic emission source based on time difference of arrival," in 2021 Signal Processing Symposium (SPSympo), 2021.

[21]. H. Yuan, Y. Xia, and H. Yang, "Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack," IEEE Trans. Syst. Man Cybern. Syst., vol. 51, no. 11, pp. 6926–6937, 2021.

[22]. T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and fitness data management using the IoT-based blockchain platform," J. Healthc. Eng., vol. 2021, p. 9978863, 2021.