ISSN 2007-9737

Survey of Mobile Cloud Computing Security and Privacy Issues in Healthcare

Rabab M. Nabawy[1,2,*], Mohamed Hassan-Ibrahim[1], Mostafa Rabee-Kaseb[1]

[1] Fayoum University, Computer Science, Fayoum, Egypt

[2] October 6 University, Computer Science, Egypt

{rm2227, mhi11, mrk00}@fayoum.edu.eg

Abstract. Wireless positioning is regarded as an essential research direction across various domains. There are several wireless positioning algorithms available, with two-step positioning methods being the most significant. In order to increase positioning accuracy and efficiency, standard two-step positioning algorithms extract measurement data from the received signal, such as angles of arrival (AOA), times of arrival (TOA), and time differences of arrival (TDOA). The omnipresent healthcare system can benefit from the effective solutions offered by wireless sensor networks. A key element of the healthcare system of the future is the wireless sensor network. Cloud computing (CC), fog computing (FC), Internet of Things (IoT), and telehealthcare technologies are utilized in the healthcare industry to facilitate data sharing across diverse stakeholders. Healthcare data infringement might result from an unsafe healthcare method, giving hackers complete access to patient email addresses, messages, and reports. On the other hand, a secure method for healthcare 4.0 can raise stakeholder, patient, and caregiver satisfaction. These facts serve as the foundation for this study, which offers an extensive literature evaluation of several security issues and privacy-related healthcare concerns. Challenges and future research directions for achieving security and privacy in healthcare will be presented.

Keywords. Cloud computing, internet of things (IoT), geographical positioning system (GPS), security, privacy.

1 Introduction

The medical field offers a program "to keep people healthy," which helps patients survive [1]. Both improving the diagnostic process utilized in healthcare and developing the technologies employed by healthcare professionals can help achieve this goal.

There have been several developments in the healthcare field. 1.0 to 4.0 for medicine. Healthcare 1.0 permits doctors to maintain handwritten patient medical history records.

In contrast, these handwritten records were superseded by electronic records in Healthcare 2.0. Healthcare 3.0 uses wearable devices (W.D.s) to track patient medical history in real-time [2]. In the end, an electronic health record (EHR) system was created that enables patient data to be kept in a database repository that enables accessing it from anywhere in the world over the Internet.

Protecting patient privacy is one of the most significant part of making sure of data integrity. Healthcare 4.0 will save patient data in the centralized HER system, which continually monitors patients' health information and offers real-time services to patients [3].

Wearable technology and medical devices that are implanted in people can both be used to track their health. W.D.s are equipped with a variety of medical sensors, a procedure known as telehealthcare, to get the patient's blood pressure, heart rate, temperature, and glucose level remotely and keep them in the centralized HER [4].

Understanding the patient's behaviour is the major duty in order to deliver better remote patient care. IoT and telehealthcare can collaborate to manage illnesses more effectively [5].

Health monitoring, autonomous driving, smart grids, smart homes, intelligent transportation systems, smart devices, and mobile device (robot) placement are only a few of the many positioning services presented by the intelligent society [1-2]. WSN is growing in popularity across a wide range of sectors and is receiving greater attention in research as the Internet of Things (IoT) expands.

Furthermore, because the GPS method cannot meet requirements in an inside environment, the WSN methodology may make up for GPS's shortcomings and provide accurate localization services. Localization is achieved by determining and measuring the interspace between the mobile terminal and sensor nodes. Using distance measurements, such as received signal strength (RSS) [5, time of arrival (ToA) [3, time difference of arrival (TDoA) [4, angle of arrival (AoA) [6, etc., a range-based localization technique finds locations.

1.1 Scope

Numerous studies have been conducted to draw attention to the security and privacy concerns with healthcare 4[3]. The majority of these studies highlight privacy and security issues and how different healthcare sectors have addressed them. We have outlined the many Healthcare 4.0 application areas in the recommended evaluation and spoken about how integrating more technologies may benefit the healthcare sector. The confidentiality and privacy of the patient's medical data are guaranteed by this integration, which also improves diagnosis. Healthcare IoT presents both potential and constraints, as exemplified by Baker et al. [24]. Attacks against EHR systems were surveyed by Priya et al. [22], with a focus on known security flaws.

1.2 Contributions

The review presents in detail security and privacy concerns in healthcare. We highlight many open problems and challenges for privacy and security. The next section represents the main parts of this review:

– The background and the need for both security and Privacy in Healthcare 4.0.
– Merits and demerits of security and Privacy in Healthcare 4.0.
– Different techniques that are used to improve security and Privacy in Healthcare 4.0.
– The categorization of various security and privacy methods.

2 Background

2.1 Classification of Localization

Within this area, we presented indoor localization techniques for smartphones that were categorized based upon the different methods used by various studies [1]. They are categorized as Path Loss Prediction, Dead Reckoning, and Mapping. These approaches may employ one or more of the measurement strategies covered in the preceding section, and they may have made use of one or more smartphone sensors or components for position estimation.

2.2 Mapping

Fingerprinting, another name for mapping [2], is the process of creating a model of signal intensity. By comparing the detected signal intensities to the previously stored locations on the map, the approach estimates the position of the mobile device. The offline phase and the online phase are two stages.

2.3 Path-loss Prediction

A smartphone's estimated position may also be determined by figuring out how far away it is from three B.S. or A.P. using different signal propagation route loss models. A.P. may receive signals from a device that takes distinct routes and experiences absorption, deflection, or reflection.

2.4 Dead Reckoning

This method calculates an object's ultimate location by estimating its speed over a certain distance and time, and it uses a previously calculated position that was acquired by measuring some external references, such as a GPS, to

assess an object's present position [2-4]. Step event detection, heading direction estimate, step length computation, and position estimation are its four stages.

3 Wirelessly Networked Sensors in Healthcare

Wireless network sensors suggest sampling physiological, behavioural, cognitive, and physical processes that differ across individuals, buildings, and even bigger ones. Applications in healthcare based on sensory input create such massive sampling over spaces of different sizes [1]. Information is gathered from several dispersed sensors.

In addition, the sophistication of sensing has increased tremendously with the development of inexpensive, immature sensors; however, high-quality sensors are needed for home and personal use, as well as the creation of complex machine learning algorithms that allow complex conditions like stress, depression, and addiction to be extracted from sensory data. Lastly, the evolution of ubiquitous Internet connectivity has made it easier for caregivers to receive sensor data on time. We present a list of these technologies' uses in healthcare in the sections that follow.

4 Issues in Localization

When it comes to WSN localization, localization accuracy is the most important factor to consider since, without it, WSN is useless. A detailed description of a few more problems that significantly impact WSN may be found below.

4.1 Accuracy

WSN accuracy is crucial for the majority of localization applications [13]. The accuracy becomes higher in this instance by calculating the distance between two nodes using Euclidean measurement.

4.2 Energy Consumption

Given that WSNs have limited resources, energy consumption is a critical concern. WSN is made up of tiny sensors with changeable or limited-energy batteries that cause problems for the network when they run low [2]. The transfer of data uses more energy. Energy is needed even when the sensors are not in use.

4.3 Overhead

The costs of the sensor nodes include expenses for hardware, processing, and communication incurred by the sensor nodes are included in the overhead of localization techniques. A big, effective data structure is needed for localization in a 3D network [1].

4.4 Optimization

Every area of human endeavour and every computer science engineering research project involves some degree of optimization [4]. Biologically driven computational techniques, such as artificial bee colony (ABC), genetic algorithm (G.A.) [5], particle swarm optimization (PSO) [1], and differential evolution (D.E.) [2], are integrated into localization methods.

4.5 3D Deployment

Traditionally, localization has meant figuring out where the 2D WSN sensor node is. Nevertheless, it is used in 3D in different contexts, including environment monitoring, space exploration, surveillance, and undersea ecosystems [22].

4.6 Security and Privacy

In many applications, privacy and data security are considered the major concerns. The Internet of Things and related services are growing quickly, and this is one of the key drivers.

This may lead us to consider a number of issues, including the authentication protocol. It's also essential to examine current assaults and their defences. Thus, the identical behaviour is seen by the authentication point.

The majority of the studies concentrate on the authentication process between the tags and the reader, showcasing novel approaches to safeguard this communication versus numerous known attacks; similarly, the ownership transfer topic showcases novel approaches to enforce security during the actual tag transfer, protect the parts' privacy, and investigate the process' scalability to secondary markets.

In order to stop an attacker from pretending to be someone else or from violating the shared authentication procedure, security concerns have to be taken into serious consideration.

4.7 Security Measures

IoMT is now confronted with several security challenges, including inadequate security and privacy protocols as well as a lack of awareness and training. There are multiple categories that separate cryptographic and non-cryptographic solutions. Five tiers of security solutions will be offered in order to identify and avert threats.

Additionally, to protect patient privacy and lessen the harm caused by these known assaults. By providing physical flexibility and mobility, patients' health will be monitored in real-time.

4.7.1 Non-technical Security Measures

Non-technical security measures ensure the securing of the medical information of the patients and also train the staff; training the medical and I.T. staff could be carried out in three different ways:

a. Raising Awareness,
b. Technical Training,
c. Raising the Education Level.

4.7.2 Technical Security Measures

Using an end-to-end secure Internet of Medical Things system for the adoption of technical security solutions needs to be the first priority.

– Authentication and Certification Using several variables: A strong authentication and verification process has to be in place to safeguard IoMT systems against unwanted access. There is a vast array of biometric techniques, which are classified into physical and behavioural processes. For example, these include: • Physical biometric techniques, such as iris or retinal scans or facial recognition software.

– Cognitive, movement, speech, keyboard, mouse, and other behavioural biometric techniques, as well as signature recognition and other biometric techniques, are also used.

– Multi-Factor Authentication Techniques: By establishing authentication first, you can confirm the authenticity of both the source and the destination.

– Authorization Techniques: The minimal privilege has to be used for authorization.

– Techniques for Availability: To ensure constant data flow, servers must be maintained.

Honeypots: Systems that utilize them must be able to identify attackers along with their tools, goals, and techniques in order for them to be effective.

5 Taxonomy of Security and Privacy in Healthcare

The global taxonomy of security and privacy issues in Healthcare 4.0 concerns machine learning (ML), W.D., IoT, telehealthcare, policy, scheme, and network traffic-based security and privacy issues in healthcare. The proposed classification is shown in figure1.

5.1 Processing-based Schemes

The speedy growth of technology in the field of information and communication integrates a huge amount of data, which we call B.D.

This marvellous amount of data transmitted over the Internet, which is an open channel, and to manage security attacks, is a main challenging issue in processing-based techniques like CC, F.C., and Mobile edge computing (MEC) [15].

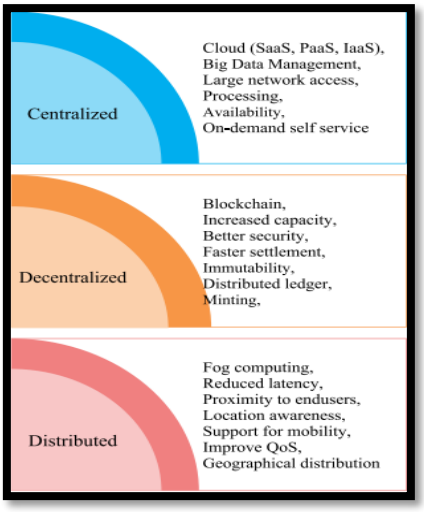

Fig.1. Proposed taxonomy of healthcare security

5.1.1 Distributed Scenario

Users store data on their local storage so that only one user can access it. In case of hardware failure, it becomes difficult to recover data from the server. With a distributed system, such a problem can be easily solved, while other machines can process the request to avoid the request failure.

5.1.2 Centralized Scenario

Nowadays, a significant volume of data is being produced as conventional systems cannot handle the vast amount of information. This is because of advances in technology. Therefore, effectively overseeing and regulating it can be difficult duties that can be accomplished with the help of a framework such as the cloud.

Zhou and colleagues [58] created a dynamic method for mining medical texts and extracting image features in the cloud healthcare system while ensuring privacy. It decreases the expense of computing and sending data while enhancing the security of input and output data.

5.1.3 Decentralized Scenario

Creating a decentralized system is essential nowadays to build trust among all parties in a multiparty network [15]. The institution-driven approach emphasizes the sharing of information among different business organizations, such as various hospital organizations. In a setting where patients are in control, stakeholders have access to the patient's EHR data via APIs.

The evaluation of blockchain security was conducted by analyzing five elements: data aggregation, digital access regulations, data liquidity, immutability, and patient identity [16].

5.2 Machine Learning-based Schemes

The common use of cloud, mobile, online, and IoT technologies raises the risk of security breaches. ML picks up on cues from its surroundings and handles complicated scenarios with ease. It is noticed that the scientific method with the greatest degree of adaptability and finds usage in a widespread of fields, including image processing, security, autonomous driving, and network intrusion detection. Additionally, it may be applied to the prediction of illnesses using various datasets.

5.3 Wearable Device-based Schemes

Wearable devices (WDs) are gadgets that individuals wear to monitor health data like sleep patterns, heartbeat, blood pressure, body temperature sensors, and exercise data. It aids in enhancing the patient's quality of life. Data produced by W.D. is transmitted to the patient's Mobile using various communication channels like blue-tooth and zig-bee, as shown in Figure 2.

6 Related Work

Localization is the act of identifying the geographic position of a user or device. The process may involve identifying a user and tracking their movement, or it may not. Therefore, the proposal could identify areas of focus for isolation and gradual economic resurgence.

Experts recommended the use of a sensor network that utilizes lightweight remote sensor hubs equipped with IoT technology to communicate information through distributed computing. Therefore, they adhere to privacy and security protocols to access the patient care

system and maintain the confidentiality of information. In e-health systems, experts studied combining IoT and cloud computing, identifying and outlining relevant hurdles, prospects, and constraints.

They provided evidence of the crucial nature of e-Health platform security and suggested a validation approach for obtaining e-Health frameworks with consistent deployment. Current surveys were examined in order to analyze the most efficient methods for protecting patient medical records.

Numerous research studies and experiments on mobile phone localization are currently being conducted in the healthcare community. It has the ability to monitor every alteration in the area. Examined were recently published papers showcasing innovative techniques for localization. Their attention to detail, research field, method of categorization, and methods of comparison were observed and understood.

In the article Akbarzadeh et al. (2021) [14], simple positioning methods without an emphasis on precision are introduced. As a result, BLE-based solutions enable lower installation costs and power consumption. However, this depends on the essential neighbourhood commercial services, like iBeacon. When anticipated systems are supposed to work on par with proximity-based ones, their functionality is limited.

The required accuracy for a restricted set of tests proposed that the suggested system outperforms a remote solution in terms of performance. In addition, little tweaks that reduce power consumption can be applied to systems like Wi-Fi. Unfortunately, limitations in the available technology make it impractical to perform a full power consumption measurement. Two cells are being used in the test.

The recommended fix enables a multi-year battery life extension for the beacons. This study's theoretical contribution, which suggests a mobile app for effective hospital administration, seeks to improve the body of existing research. Consequently, in order to improve hospital amenity management, the recently developed platform analyzes data on structures, their clients, and the period of their visits. In addition, by keeping an eye on available space and automatically modifying lighting and temperature to maximize energy

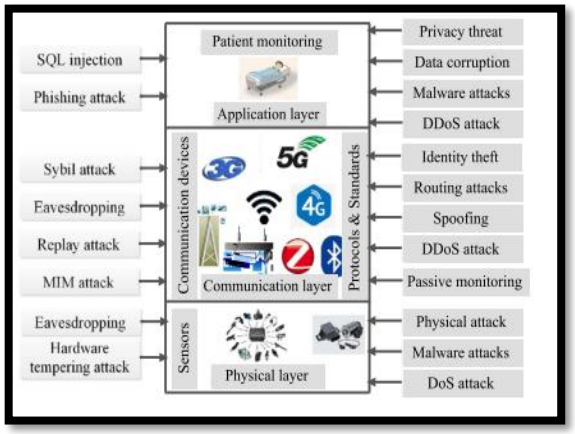

Fig.2. Possible attacks on a different layer

efficiency, the present system's characteristics may be improved.

Nasr et al. (2021) [15] consider smart healthcare guarantees the effectiveness of healthcare when compared to other options. Providing healthcare facilities with affordable services through a straightforward and safe process efficient and affordable system for monitoring health.

The study looked at cutting-edge wearables and smartphones that might monitor basic health information, use machine learning to identify COVID-19, diabetes, and heart disease, and provide support to older people living in their homes.

This review emphasizes the importance of software integration frameworks in creating smart healthcare systems. We have evaluated the benefits and drawbacks of several options. We also spoke about the primary issues that contemporary healthcare systems need to resolve in order to create efficient support models. Suggested new lines of inquiry to improve the current healthcare infrastructure.

Technology may help medical professionals by bringing new organizational structures, even if they cannot replace the medical system entirely. By working together on a common platform, researchers and medical professionals may create assistance solutions.

The article Soares Silva et al. (2021) [17] examined how cities in a heavily affected state in Brazil were

cut off by analyzing networks formed by mobile phone location data. By using mobility thresholds, clusters are formed to analyze the behaviour of 192 cities before and after the enactment of social distancing regulations. Thus, it was possible to witness the towns with varying degrees of connectivity.

The weighted flow-based clustering situations are a part of what this method offers; they could assist policymakers in determining if they should isolate a lone city or a cluster of cities with border regulations. One of the study's additional enhancements is cluster risk assessment. It involves prioritizing factors from most crucial to least crucial based on selected risk measures and specific circumstances.

When economic recovery measures are implemented, isolated clusters without instances may receive preferential treatment. As a result, economically sustainable clusters can be established to maintain both strong and weak connections between cities.

Our proposal aims to collect data for policymakers to determine areas for isolation and economic recovery, taking in consideration epidemiologists' views. Epidemiologists must determine isolation protocols, criteria for lockdowns, and reopening regions based on the timing of infections and the availability of healthcare facilities. Future research projects might include modifying clustering techniques to analyze small-world effects in weighted directed graphs.

In this case, different groups can be distinguished and analyzed without requiring specific flow minimums to alter the original graph structure. Additionally, the risk assessment could involve data regarding the hospital's specific location within each city or region. Furthermore, this article analyzes various states in Brazil.

This article Horng and Chen (2021) [18] suggested a fuzzy theory-driven adaptive threshold algorithm to detect the fall. If a fall happens, Beacon quickly detects where the caregiver is and sends information about the fall's location and identity via Wi-Fi to the server. Notifications are then sent to the caregiver's mobile app through the server. The system allows current healthcare providers to access additional real-time data and feedback, resulting in enhanced service quality and efficiency, leading to reduced human costs and resource usage.

The research Rhayem et al. (2021) [19] was conducted and put into practice with the aim of monitoring healthcare, which can be keept track of elderly individuals with chronic illnesses, pregnant women, and individuals with disabilities. These situations are connected to the ongoing changes in limitations and demands for the deployment of MCOs (time, place, condition). Additional information from the patient's medical record should be taken into consideration in order to guarantee a more accurate and appropriate treatment.

This article investigates the problem and presents a contextually aware system (IoT Medicare system) utilizing semantics to monitor patients with MCOs. The main domain ontology (HealthIoT-O) is applied to define the meanings of different MCOs and their data in the system.

The article McConville et al. (2021) [20] presented Vesta, a cutting-edge, reasonably priced digital health platform designed to track patients' whereabouts, health, and overall well-being in detail.

The platform's "smart home in a box" concept was deliberately designed to be more cost-effective than other systems, which added to its widespread appeal as an approachable tool for data collecting. It described how Vesta combined important data with the house by gathering accelerometer data from a wrist-worn wearable device with RSSI readings from four sites. The analytics system examines activity, interior positioning, and sleeping patterns in the smart home to transform raw sensor data into meaningful knowledg by using data science and machine learning.

In order to evaluate Vesta's efficacy, two case studies were looked at: one included patients having heart valve surgery, and the other featured a group of twenty patients. Three distinct periods of patient behaviour and activity at home—one prior to surgery and two following—could be seen on the platform.

The results were confirmed using a tailored survey including questions on physical activity and sleep quality, as well as standardized clinical Patient-Reported Outcome Measures (PROMs). The suggested platform has the potential to

enhance the clinical evaluations by incorporating quantitative health data from popular home monitoring devices into digital health research.

In Amine et al. (2021) [21], this system's primary flaw is that it may be used for more than just patient monitoring; machine learning can be suggested for classifying data. Because it may assist diabetic patients, their families, physicians, and medical researchers in making decisions about their care based on large data sets, predictive analytics is particularly important for diabetes patients. This research discusses predictive analytics utilizing four distinct machine-learning algorithms and outlines a new approach for monitoring diabetes patients.

Singha and Chatterjee (2021) [22] put forth a privacy-preserving paradigm in which various entities communicate with one another inside this architecture to carry out certain functions, including gathering, aggregating, storing, and analyzing data while maintaining data privacy. Below is a description of each entity:

- Smart User: People who are smart may also be healthy. Patients in their later years, those in critical condition, hospital patients, physicians, nurses, lab technicians, etc. In order to detect biosignals, people have had bio-sensors implanted in their bodies. Subsequently, they are combined in Internet of Things devices and protected cloud storage.
- Edge Gateway: This smart gadget is in charge of locally processing little data collected from the community of smart patients. Smart equipment such as oxygen delivery systems and cardiac pumps are controlled by means of this local diagnosis of data. In addition, it encrypts the data, puts it in cloud storage for more research, and allows physicians to access it for patient care.
- Database Manager: This manager is in charge of processing queries and storing data. The encryption key from the key generator will be searched using the processed query.
- Server Edge. This will handle all data resources from various intelligent community members and group them into various clusters for encrypted analysis.

Sivan R and Zukarnain (2021) [23] suggested a method for encrypting and securing identity-based data exchange. Many options were provided to secure data stored in cloud-based e-health systems, making use of existing PKE, IBE, IBBE, and ABE methods. To safeguard data security, an appropriate security solution needs to be created and kept up to date. Additionally, they emphasized a thorough analysis of current cloud-based e-health systems that use both non-cryptographic and cryptographic methods in order to safeguard the security and privacy of digital data.

Kondaka and Thenmozhi (2021) [24] suggested the method, known as iCloud-assisted Intensive Deep Learning (iCAIDL), which unites two potent techniques into one cohesive system. Our initial approach involves utilizing the Internet of Things in conjunction with the Cloud Paradigm to facilitate communication and interaction between our suggested smart device and distant servers.

The cloud paradigm offers sufficient storage capacity contingent on data needs and the number of patients or senior citizens. The second tactic involves utilizing machine learning techniques in conjunction with the Cloud IoT paradigm to anticipate challenging circumstances for patients. This allows medical professionals or other caregivers to take appropriate action in response to the event.

The suggested iCAIDL logic makes it possible for the end user to identify patient or elderly people's health records in a more thorough way without worrying about human error. Additionally, all metrics are fully transparent to the doctor and caregivers' end for additional norm verification.

Viswanathan (2021) [25] proposes using an energy-harvesting healthcare IoT system to improve download speeds and local computation without compromising data security, IoT efficiency, or high-level computing models. The system utilizes a data protection allocation scheme that is based on RL. This plan assesses the level of anonymity, energy consumption, and measurement delay to establish the download protocol. The RL-powered offloading strategy employs a transition learning technique, an acknowledged radio channel model, and Dyna architecture to accelerate learning for complex healthcare systems in DIT.

In Aitzaouiat and Latif (2021) [26], in order to convert between different nodes, such as the Hospital Information System (HIS) HTTP/TLS

protocol and the CoAP/DTLS protocol, the suggested approach uses a model as an integrated IoT/WEB proxy security.

The suggested method carried out better than existing approaches for many reasons: It is a secure prototype implementation that fulfils the following requirements: a) it makes use of a hierarchical collection of machine learning and prediction algorithms; b) it is user-friendly, open-source, and interoperable; c) it uses the correlation criteria to achieve a greater accuracy rate.

AlZubi and Al-Maitah (2021) [27] proposed that cognitive machine learning facilitates safe healthcare data exchange by supporting the attack detection architecture. Cloud storage of the gathered data will be facilitated by the Healthcare Cyber-Physical Systems. Cyber-attack behaviour is predicted by machine learning algorithms, and analyzing this data might help medical professionals make decisions.

The basic foundation of the suggested method is a patient-centric design that protects data on a reliable device, such as the end users' smartphones and gives them a choice over data-sharing access. According to experimental data, the proposed model outperforms other current models with an attack prediction ratio of 96.5%, an accuracy ratio of 98.2%, an efficiency ratio of 97.8%, a shorter latency of 21.3%, and a communication cost of 18.9%.

Through the integration of natural language capabilities, extensibility tools, compliance constructs, and integrated medical intelligence, Kumar Prasad et al. (2021) [28] have made it possible for healthcare organizations such as payers, providers, pharmacies, HMOs, and telehealth to give people access to reliable and pertinent healthcare information and services.

Bots with anomaly detection systems have further advantages over healthcare systems. This study employs the C2B-SCHMS framework, which uses machine learning isolation graph techniques to find any anomalies in the dataset. Because of this, cloud computing for medical services will be reliable.

Farrokhi and Farahbakhsh (2021) [29] gives a worldwide overview of the real issues with smart fitness and their fixes. In order to achieve this, three areas of smart fitness have been examined: artificial intelligence, social IoT, and IoT-based solutions (such as fitness trackers, fitness applications, and movement analysis). In terms of practical solutions and designs pertaining to IoT-based solutions, an AI-based recommendation accompanied by a comprehensive monitoring system remains challenging. Artificial intelligence (AI) in smart fitness is used for tasks including extracting exercise aspects, forecasting diets and workouts, preventing injuries, and overtraining.

Additionally, social IoT is a crucial component of the smart fitness space that may enhance knowledge of smart fitness through the sharing of experiences with different solutions, sensor kinds, techniques, and individuals with varying cultural backgrounds, socioeconomic statuses, and even personal habits. Smart Fitness may function as a coach's squad of assistants, assisting in improved decision-making.

It should be able to handle training information history management, workout and diet prediction monitoring, user authorization and identification, and fitness big data analysis in order to be a comprehensive and perfect smart fitness solution. There is still a lot of room for improvement when it comes to smart fitness.

In order to calculate the distance between a beacon node in an indoor setting and a mobile node carried by Alzheimer's patients, the study by Munadhil and Gharghan (2021) [30] proposed two route loss models. Because of the building's restricted space, the tested distance could only be 26 meters. Because of its robust characteristics and features compared to other wireless technologies, the ZigBee wireless protocol was adopted.

In trials with volunteers to verify the algorithm's accuracy, patients with high fall risk, such as those with diabetes, stroke, physical disabilities, and osteoporosis, are recommended. The ageing population is taken into account in this study, which calls for more investigation.

Yi and Feng (2021) [31] created and demonstrated a method for gathering online information on lower-limb kinematics and kinetics. Specifically, continuous prediction of movement is carried out by combining EMG and IMU signals, leading to the development of a real-time capable inverse dynamic model.

This method offers a thorough prediction of kinematics and kinetics in a specific motion mode,

addressing issues with PR-based motion intent recognition methods. Furthermore, by taking into account the impact of EMD, a forecast is made prior to actual movement in order to address the algorithm's computational time. Therefore, this technique offers fundamental information on walking patterns for smart healthcare applications, such as remote diagnosis and monitoring of diseases.

Hamad and Dawod (2022) [31] focus on the primary implementation framework for Elastic Mobile Cloud Computing (EMCC) solutions, covering cloud setup, program dissemination, module extraction, module transmission, program execution, and outcome. Then, the article examines the primary data security concerns regarding users' mobile devices that were emphasized by EMCC: data stream interception and privacy deficiencies. This implies that utilizing risk management can lessen security risks linked to implementing EMCC programs. Assessing the risks related to each distribution method is crucial in order to accomplish risk management. They created a method to quantify risk for the EMCC modular task, enabling them to effectively overcome the primary challenge of the approach.

Kiani and Shahid (2022) [32] highlight potential causes of data leaks, including in-law disputes, subpar equipment, ignorance, and the absence of specialized local law enforcement. This article addresses IoHT device compliance difficulties with relation to healthcare data privacy and protection legislation, bringing attention to the rising need for a proper regulatory framework. Additionally, the research gives some solutions for enhancing the secrecy and security of IoHT implementation.

To meet the needs for mutual authentication and protect user anonymity, Nag and Chandrakar (2023) [33] developed a remote user authentication system based on smart cards. An automated validation Internet Security Protocol Application (AVISPA) has demonstrated through simulation that the proposed system can fend against both passive and aggressive physical threats. According to an informal security evaluation, the developed scheme is resistant to a variety of assaults; compared to analogous existing protocols, the recommended protocol exhibits more security characteristics and is more complicated in calculation cost, execution time, and communication cost.

In the apper Thatikonda and Padthe (2023) [34], there are two categories in the suggested method. The initial part of the paper explores the technique of data formulation modification to understand data correlation and assess variables using trained data. It helps to achieve both the development of data scale and data minimization. By using the subset selection to show the model's fitness based on the data, the selection feature is employed in the second section to validate the model. Additional examples of various Android applications are required in order to analyze the framework with respect to metrics such as data accuracy and F-measure. This work focuses on Chi-square, Gain Ratio, information gain, logistic regression analysis, One R, and PCA since feature selection is thought to be a problem.

Prabha and Kanagasabapathi (2023) [35] employ capacity tools and layered, private, information-nature-driven encryption approaches like MES, which use safe health information exchange. Comparative results show that, in the Cloud Environment (from numerous execution factors), this strategy works better than other well-liked strategies. The ensuing list includes some likely obstacles and outcomes of the proposed project.

In the work Nyangaresi (2023) [36], wireless body area networks have been used to gather and send patient health data to hospital medical specialists for review from a distance. Since the transmission takes place over the open Internet, this procedure opens the door to several attacks. They examine the recent history in order to make this situation better. It has been demonstrated, therefore, that a large number of these techniques have significant communication and computation costs.

Furthermore, the majority of these existing protocols are insecure due to inherent flaws. This work presents the development of a three-factor security mechanism that combines passwords, smart cards, and biometric data to overcome these issues. The ROR model and BAN logic were used to provide formal security, and the outcomes showed it was safe.

7 Conclusion

Performance metrics and security and privacy regulations must be adhered to by digital services. Hence, building resilience to cyberattacks is crucial for improving the filtering skills of users of applications. Smart healthcare provides a cost-effective health monitoring system that is portable, secure, and efficient.

This enables people to receive high-quality medical treatment at a more affordable price compared to the rates of hospitals and nursing facilities. This study briefly looked into wearables and mobile phones for using machine learning to monitor vital signs. Various systems are incorporated within software integration frameworks. Moreover, we discussed the main challenges associated with the latest smart healthcare systems, which are the main obstacles in developing working prototypes.

Future research should explore specific strategies to further enhance the safety of the healthcare system. Even though technology cannot fully take over the healthcare system, it can help alleviate some of the workload for healthcare professionals by providing certain services and systems. Collaboration between scientists and medical professionals can lead to the development of assistive technologies that offer a foundation.

8 Challenges and Future Research Directions

Even if several assistive frameworks that highlight smart healthcare have been enhanced with the help of contemporary technologies, certain issues must be resolved to highlight a scalable, safe, conveniently accessible, and effective healthcare system. Combining data from various sensors is a significant obstacle to deploying wearable technology, such as smartphones, in the context of smart healthcare.

For health monitoring applications, it is crucial to transform the signals from diverse sensors attached to patients into a useful format because the numerous sensors provide several kinds of data. Future research can look at a number of data fusion approaches for combining information from multisensory devices in order to provide simplified signals that increase dependability and reduce the amount of bandwidth needed for connection with the cloud layer.

Different security protocols, like Blockchain, will retain more security and privacy and are advised to provide safe data exchange between users. Therefore, it is critical that these three factors be taken into consideration when developing AAL systems and that future research with older persons adhere to user-based testing and improvement. Last but not least, privacy and security issues pertaining to health-related data are crucial. Therefore, these elements need to be incorporated early on into the design of smart healthcare frameworks, making use of the most recent ones.

References

1. **Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., Sadoun, B. (2019).** Habits: blockchain-based telesurgery framework for healthcare 4.0. 2019 international conference on computer, information and telecommunication systems (CITS) IEEE**.** pp. 1–5. DOI: doi: 10.1109/ CITS.2019.8862127.
2. **Hathaliya, J. J., Tanwar, S., Tyagi, S., Kumar, N. (2019).** Securing electronics healthcare records in healthcare 4.0: A biometric-based approach. Computers & Electrical Engineering, Vol. 76, pp. 398–410. DOI: 10.1016/j.compeleceng.2019. 04.017.
3. **Coventry, L., Branley, D. (2018**). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, Vol. 113, pp. 48–52. DOI: 10.1016/j.maturitas. 2018.04.008.
4. **Shankar, K., Lakshmanaprabu, S. K., Khanna, A., Tanwar, S., Rodrigues, J. J., Roy, N. R. (2019).** Alzheimer detection using Group Grey Wolf Optimization based features with convolutional classifier. Computers & Electrical Engineering, Vol. 77, pp. 230–243. DOI: 10.1016/j.compeleceng. 2019.06.001.
5. **Gupta, R., Tanwar, S., Tyagi, S., Kumar, N. (2019).** Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions.

IEEE network, Vol. 33, No. 6, pp. 22–29. DOI: 10.1109/MNET.001. 1900063.

6. **Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Maasberg, M., Choo, K. K. R. (2018).** Multimedia big data computing and internet of things applications: A taxonomy and process model. Journal of Network and Computer Applications, Vol. 124, pp. 169–195. DOI: 10.1016/j.jnca.2018. 09.014.
7. **Mannay, K., Benhadjyoussef, N., Machhout, M., Urena, J. (2016).** Location and positioning systems: Performance and comparison. 2016 4th International Conference on Control Engineering & Information Technology, IEEE, pp. 1–6. DOI: 10.11 09/CEIT.2016.7929105.
8. **Rhayem, A., Mhiri, M. B. A., Drira, K., Tazi, S., Gargouri, F. (2021).** A semantic-enabled and context-aware monitoring system for the internet of medical things. Expert Systems, Vol. 38, No. 2, p. e12629. DOI: 10.1111/exsy. 12629.
9. **Shuaieb, W., Oguntala, G., AlAbdullah, A., Obeidat, H., Asif, R., Abd-Alhameed, R. A., Kara-Zaïtri, C. (2020).** RFID RSS fingerprinting system for wearable human activity recognition. Future Internet, Vol. 12, No. 2, p. 33. DOI: 10.3390/fi12 020033.
10. **Ghayvat, H., Awais, M., Gope, P., Pandya, S., Majumdar, S. (2021).** Recognizing suspect and predicting the spread of contagion based on mobile phone location data (counteract): a system of identifying covid-19 infectious and hazardous sites, detecting disease outbreaks based on the internet of things, edge computing, and artificial intelligence. Sustainable Cities and Society, Vol. 69, p. 102798. DOI: 10.1016/j.scs.2021.102798.
11. **Mohammad, G. B., Shitharth, S. (2021).** WITHDRAWN: Wireless sensor network and IoT based systems for healthcare application. DOI: 10. 1016/j.matpr.2020.11.801.
12. **McConville, R., Archer, G., Craddock, I., Kozłowski, M., Piechocki, R., Pope, J., Santos-Rodriguez, R. (2021).** Vesta: A digital health analytics platform for a smart home in a box. Future Generation Computer Systems, Vol. 114, pp. 106–119. DOI: 10.1016/j.future. 2020.07.046.
13. **Yi, C., Jiang, F., Bhuiyan, M. Z. A., Yang, C., Gao, X., Guo, H., Su, S. (2021).** Smart healthcare-oriented online prediction of lower-limb kinematics and kinetics based on data-driven neural signal decoding. Future Generation Computer Systems, Vol. 114, pp. 96–105. DOI: 10.1016/j.future.20 20.06.015.
14. **Akbarzadeh, O., Baradaran, M., Khosravi, M. R. (2021).** IoT-Based smart management of healthcare services in hospital buildings during COVID-19 and future pandemics. Wireless Communications and Mobile Computing, Vol. 2021, No. 1, p. 5533161. DOI: 10.1155/2021/ 5533161.
15. **Nasr, M., Islam, M. M., Shehata, S., Karray, F., Quintana, Y. (2021).** Smart healthcare in the age of AI: recent advances, challenges, and future prospects. IEEE Access, Vol. 9, pp. 145248–145270. DOI: 10.1109/ACCESS. 2021.3118960.
16. **Parvathy, V. S., Pothiraj, S., Sampson, J. (2021):** Automated internet of medical things (IoMT) based healthcare monitoring system. In: Hassanien A.E., Khamparia A., Gupta D., Shankar K., Slowik A. (eds) Cognitive Internet of Medical Things for Smart Healthcare, Studies in Systems, Decision and Control, Springer, Vol. 311, pp. 117, DOI: 10.1007/ 978-3-030-55833-8_7.
17. **Silva, J. C. S., de-Lima-Silva, D. F., Neto, A. D. S. D., Ferraz, A., Melo, J. L., Júnior, N. R. F., de-Almeida-Filho, A. T. (2021).** A city cluster risk-based approach for Sars-CoV-2 and isolation barriers based on anonymized mobile phone users' location data. Sustainable cities and society, Vol. 65, No. 102574. pp. 2210–6707, DOI: 10.1016/j. scs.2020.102574.
18. **Horng, G. J., Chen, K. H. (2021).** The smart fall detection mechanism for healthcare under free-living conditions. Wireless Personal Communications, Vol. 118, No. 1, pp. 715–753. DOI: 10.1007/s11277-020-08040-4.
19. **Rhayem, A., Mhiri, M. B. A., Drira, K., Tazi, S., Gargouri, F. (2021).** A semantic-enabled and context-aware monitoring system for the internet of medical things. Expert Systems, Vol. 38, No. 2, p. e12629. DOI: 10.1111/exsy. 12629.

20. **McConville, R., Archer, G., Craddock, I., Kozłowski, M., Piechocki, R., Pope, J., Santos-Rodriguez, R. (2021).** Vesta: A digital health analytics platform for a smart home in a box. Future Generation Computer Systems, Vol. 114, pp. 106–119. DOI: 10.1016/j.future. 2020.07.046.
21. **Rghioui, A., Lloret, J., Sendra, S., Oumnad, A. (2020).** A smart architecture for diabetic patient monitoring using machine learning algorithms. Healthcare, Vol. 8, No. 3, p. 348. DOI: 10.3390/ healthcare8030348.
22. **Singh, A., Chatterjee, K. (2021).** Securing smart healthcare system with edge computing. Computers & Security, Vol. 108, p. 102353. DOI: 10.1016/j. cose.2021.102353.
23. **Sivan, R., Zukarnain, Z. A. (2021**). Security and privacy in cloud-based e-health system. Symmetry, Vol. 13, No. 5, pp. 742. DOI: 10.33 90/sym13050742.
24. **Kondaka, L. S., Thenmozhi, M., Vijayakumar, K., Kohli, R. (2022).** An intensive healthcare monitoring paradigm by using IoT based machine learning strategies. Multimedia Tools and Applications, Vol. 81, No. 26, pp. 36891–36905. DOI: 10.1007/s110 42-021-11111-8.
25. **Aitzaouiat, C. E., Latif, A., Benslimane, A., Chin, H. H. (2022).** Machine learning based prediction and modeling in healthcare secured internet of things. Mobile Networks and Applications, Vol. 27, No. 1, pp. 84–95. DOI: 10.1007/s11036-020-01711-3.
26. **AlZubi, A. A., Al-Maitah, M., Alarifi, A. (2021).** Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, Vol. 25, No. 18, pp. 12319–12332. DOI: 10.1007/ s00500-021-05926-8.
27. **Farrokhi, A., Farahbakhsh, R., Rezazadeh, J., Minerva, R. (2021).** Application of internet of things and artificial intelligence for smart fitness: A survey. Computer Networks, Vol. 189, p. 107859. DOI: 10.1016/j.comnet.2021. 107859.
28. **Munadhil, Z., Gharghan, S. K., Mutlag, A. H. (2021).** Distance estimation-based PSO between patient with Alzheimer's disease and beacon node in wireless sensor networks. Arabian Journal for Science and Engineering, Vol. 46, No. 10, pp. 9345–9362. DOI: 10.1007/ s13369-020-05283-y.
29. **Wang, Z., Rho, S., Yang, C., Jiang, F., Ding, Z., Yi, C., Wei, B. (2021).** Active loading control design for a wearable exoskeleton with a bowden cable for transmission. Actuators, Vol. 10, No. 6, pp. 108. DOI: 10.3390/act10 060108.
30. **Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., Almuhaideb, A. M. (2022).** Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, Vol. 12, No. 4, p. 1927. DOI: 10.3390/app120 41927.
31. **Nag, P., Chandrakar, P., Chandrakar, K. (2023).** An improved two-factor authentication scheme for healthcare system. Procedia Computer Science, Vol. 218, pp. 1079–1090. DOI: 10.1016/j.procs. 2023.01.087.
32. **Thatikonda, R., Padthe, A., Vaddadi, S. A., Arnepalli, P. R. R. (2023).** Effective secure data agreement approach-based cloud storage for a healthcare organization. International Journal of Smart Sensor and Adhoc Network, Vol. 3, No. 4.
33. **Sathya-Prabha, R., Kanagasabapathi, K., Sajeeth, K., Aishwarya, M. (2023).** Health information sharing in cloud environment using modular encryption standard. Recent Developments in Electronics and Communication Systems IOS Press, pp. 64–70. DOI: 10.3233/ATDE 221238.
34. **Nyangaresi, V. O. (2023).** Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks. Ad Hoc Networks, Vol. 142, pp. 1570–8705. DOI: 10.1016/j. adhoc.103117.

Article received on 29/04/2023; accepted on 06/05/2024.
**Corresponding author is Rabab M. Nabawy.*