International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

June 2024 | Issue 59 | Volume 16 | Number 2 | Pages 240-251

A COMPREHENSIVE REVIEW ON SECURED SMART HOME HEALTH SYSTEM: PROBLEMS, PROSPECTS AND ACCESSIBILITY

O.M. Almutairi [1] M.N. Yusoff [2] A.A. Bahaddad [3]

1. Computer Science Department, Shaqra University, Shaqra, Saudi Arabia, oalmutairi@su.edu.sa
2. School of Computer Sciences, University of Sains Malaysia, Penang, Malaysia, najwadi@usm.my
3. Faculty of Computing and IT, King Abdul Aziz University, Jeddah, Saudi Arabia, dbabahaddad10@kau.edu.sa

Abstract- The current healthcare and support systems are facing challenges due to the tremendous growth of the elderly population across the globe. These days, patients may remain in the relaxation of their own homes through omnipresent health monitoring via smart home technologies. This area has quickly become the leading option for the Internet of Things (IoT) and associated technologies. Healthcare innovations serve a crucial role in achieving the goals of Vision 2030 and the National Transformation Program (NTP) operating plan, ultimately enhancing the quality of healthcare in Saudi Arabia. The healthcare industry is undergoing a sea change as traditional systems embrace new technology to become smart healthcare ecosystems. Nevertheless, achieving its broad acceptance remains an aspirational goal. Even with smart healthcare systems (SHS) there are still several problems with data privacy and security, such as unauthorized access, device vulnerability, cloud storage security, authentication as well as interoperability, and regulatory compliance; to get around this, blockchain technology has come up as a practical way to make data and user privacy more secure. Blockchain has discovered many prospects in the healthcare sphere due to the flood of medical data created by electronic medical records and other ICT-based methods. This research investigates the social and technical hurdles to SHS implementation in Saudi Arabia by analyzing current expert opinions and user perceptions. The current state of the implementation of SHT in Saudi Arabia and several non-technical barriers are also discussed here. This research delves further into several SHS frameworks that use blockchain technology to enhance the system's inherent security and integrity. Finally, future research paths and blockchain application cases in the healthcare industry are highlighted.

Keywords: Blockchain, Smart Home Healthcare, Internet of Things, Data Security, Barriers.

1. INTRODUCTION

Smart home development has accelerated in recent years, posing an extensive number of data and information security problems [1]. Smart homes provide options for pleasant and secure living; they additionally help the elderly and handicapped by improving their quality of life and extending their independence at home. "Smart home health care" refers to residential health care that uses ubiquitous computing and IoT technologies [1, 2]. Such technologies offer an amazing infrastructure for healthcare reasons, allowing the aged and handicapped to get certain available healthcare treatments in the comfort of their own homes [3]. Recently, there have been cases of developed countries utilizing healthcare in smart homes and planning to utilize more SHHS in the future. SHHS has already been used in advanced nations, such as the United States, the United Kingdom, Japan, and Europe, to enhance healthcare delivery. For instance, in the United States, firms such as Philips, Qualcomm, and AT&T have built smart home healthcare mechanisms that track patients' health information and transfer the data to medical care experts [4]. In Japan, Fujitsu has launched an app that utilizes AI to track the health situations of elderly patients and inform healthcare experts of any abnormalities. In Europe, tech companies such as Tunstall, Vodafone, Epworth, and Telstra have launched SHHS, which tracks patients' situational signs and medical improvements. These examples demonstrate how developed countries have already embraced SHHS and how they are planning to utilize more SHHS in the future.

However, this is clear evidence of insufficient utilization of SHHS's applications in the undeveloped world, especially in Saudi Arabia, where SHHS remains limited research. In Saudi Arabia, the healthcare sector is advancing swiftly; consequently, there is an urgent need to embrace SHHS to enhance medical care services. Thus, it is essential to look at the causes of the limited adoption of home IoT technologies and related SHHS. According to Kichloo, et al. [5], using telemedicine and telehealth services can aid in lowering medical expenses in almost all middle eastern countries. In comparison to conventional healthcare delivery systems of Saudi Arabia, their study indicated that telemedicine and telehealth services could cut the cost of healthcare services by up to 50%. The ability of telemedicine and telehealth services to lessen the need for hospitalization and trips to emergency rooms is what accounts for this cost decrease.

Registered: 231031 | Article Info: 1803 | Accepted: 240513
Reserved: 240205 | Available: 240630

Health-related benefits can be realized when technology provides operational efficiency (comfort), monitoring and management, and consulting services. Furthermore, SHHS can lower healthcare expenses by minimizing the number of medical emergency appointments [6]. Emergency appointments with doctors are expensive, and SHHS is capable of reducing this cost by lowering patients' appointments with medical experts. SHHS can also lower healthcare expenses by fostering better drug adherence. SHHS can assist in lowering the significant cost associated with non-adherence to drugs in healthcare systems by giving patients access to remote healthcare services that can promote better medication adherence. According to Bingham, et al. [7], telemedicine services have been shown to increase medication adherence in patients with chronic conditions, including diabetes and hypertension.

In the Saudi Arabian context, SHHS can also enhance healthcare performance by enabling patients to access personalized healthcare services. Personalized healthcare services enhance patients' medical performances by matching healthcare services to the specific medical requirements of each patient. SHHS can assist patients by rendering personalized healthcare services, like medical management, disease management, and healthcare consultation that improves patients' health conditions. Smart home devices constitute a substantial portion of the consumer Internet of Things (IoT) market, but they come with inherent security risks. Security becomes a critical consideration when deploying networks on a large scale. However, privacy and security apprehensions serve as significant obstacles to the widespread adoption of Smart Home Technology (SHT). In the realm of IoT-based healthcare systems, which handle data directly linked to individuals, even information collected innocuously from wearable sensors becomes susceptible to notable privacy concerns.

SHHS adoption rates in Saudi Arabia are still low, notwithstanding the potential advantages of SHHS technologies. There are many factors that contribute to the low adoption rate, including privacy and security concerns, lack of trust in technology, perceived risk, lack of awareness and education, and the complexity of the technology. In the first place, there are anxieties about patients' privacy and security in Saudi Arabia. This is because patients are cautious about sharing their personal health data with healthcare experts in Saudi Arabia, which hampers the SHHS adoption rate in the country. One of the primary factors for the low adoption of SHHS in Saudi Arabia is privacy and security anxieties. Patients are reluctant to share their personal health information with healthcare professionals because of fears of data breaches or misuse in Saudi Arabia. According to Alshammari, et al. [8], privacy and security apprehensions are one of the primary hurdles to the low adoption of e-health services in Saudi Arabia. The research discovered that patients are anxious about the privacy of their private health data and the likelihood of it being retrieved by unauthorized private.

Before the mass scale implementation of blockchain, for ensuring privacy and security in smart health care systems, software defined networks and the finest encryption method was employed in smart cities. Also, for exchanging patient healthcare information, the best authentication approaches and access-based control systems must be employed. According to the literature of Chenthara, et al. [9] a symmetric key encryption method (SSE) is a secretly transfers data system from one entity to another. Through the use of proxy re-encryption, this architecture is able to securely communicate medical data on the cloud, ensuring that only authorized individuals are able to access it.

Blockchain technology has several applications in the field of IT for health care. Professionals created this open-source software. Compared to closed and patented software, it is more open, dependable, and quick to react to changes. Wide-ranging innovation and the ability to tailor solutions to specific requirements and demands are hallmarks of open-source software. Running on commodity hardware, blockchain technology offers cheap, high-computation. They were developed by different suppliers using open standards. They eliminate the need for complicated point-to-point data integration and are based on industry best practices due to their ease of implementation. A large number of public and commercial organizations have evaluated and approved this technology because of its safety and efficiency.

This study explores the security and privacy-related problems influencing the adoption of SHHS in Saudi Arabia. Medical care practitioners must manage these factors to enhance SHHS's adoption rates. This study goes into additional detail about the different blockchain-based architectures and how they operate to address current privacy and security concerns. At last, a blockchain based framework was also suggested which could potentially resolve the security and privacy related threats. Saudi Arabia may take advantage of the potential advantages of SHHS by fulfilling these practices, such as enhanced medical care results, decreased healthcare costs, increased quality of life, and enhanced healthcare accessibility. Despite the significance of SHHS to the Saudi Arabian, there is a shortage in the researches in this area, contributing to its low patronage in Saudi Arabia, which previous experts attributed the reason to low public enlightenment.

2. CURRENT STATUS OF AGED SOCIETY AND ELDERLY HEALTHCARE

The World Health Organization (WHO) and the United Nations (UN) categorize a society with 7% of its population aged 65 and older as an aging society, one with 14% as an aged society, and with 22% as a super-aged society. This classification is based on the percentage of the population in these age groups—their homes—there are several locations for healthcare services for the elderly. Homes for the elderly, staffed by volunteers from local healthcare institutions, are common in nations with a large elderly population. On the other hand, they may arrange for caregivers to pay regular visits to seniors living in their own homes. Here, we should see other societal circumstances in Saudi Arabia. Figure 1 displays the

changes in Saudi Arabia's population age groups (in thousands) from 1950 to 2050 [10]. There has been a noticeable acceleration in the growth rate of the age groups 60-79 and 80+. Throughout the years 1950-2015, this percentage stayed around 5%. But from now to 2050, it will grow significantly.

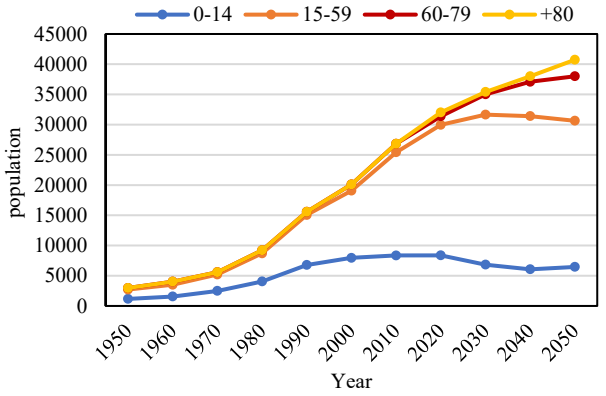

Figure 1. Generational breakdown of the Saudi Arabian population in thousands [10]

3. SMART HOME HEALTHCARE SERVICES

3.1. Fundamental Concepts of Smart Home and Related Healthcare Services

A smart linked home often includes an extensive number of interconnected electronic devices from different domains. Entertainment, energy, security, and healthcare are the four main categories into which the application sectors are often classified. From spying to catastrophic hacking, the healthcare area potentially has the broadest variety of risks. There are five types of SHHS: telemedicine, wearable technology, health information, and tailored healthcare app services.

3.2. IoT in Healthcare Services

A growing array of healthcare devices now incorporates IoT technology, becoming increasingly commonplace among the public. Individuals can track and assess their health using user-friendly wearable devices such as smart bands and watches, enabling real-time collection and monitoring of physical information. The integration of IoT technology in the healthcare sector promises cost savings, expanded remedial options, enhanced disease prevention and control, and added convenience to daily life. However, several standardization organizations and the work they have done recently on IoT standards are included in Table 1. As it can be seen in the following table, most of the organizations mainly works in energy efficiency, data security, smart and reliable architecture for implementing smart healthcare system and similar type of features.

Table 1. Organizations and their IoT-related projects

Organization	Recent IoT standards work
Internet Engineering Task Force (IETF)	• Energy-efficient features of Internet of Things protocols • Securing smart object networks
Institute of Electrical and Electronics Engineers (IEEE)	• Telecommunications and information exchange between systems • Medical device communication • Adoption of Smart Energy Profile 2.0 Application Protocol Standard
ETSI	• Reference architectures for smart body area networks and health-care • Interoperability
ITU-T	• Reference architectures for smart manufacturing, digital health, and wearable device communications
Open Connectivity	• Cloud security

However, using IoT for Saudi patients has advantages in improving patient satisfaction and experience and lowering the cost of time and effort needed to provide the best care possible for patients which is illustrated in Figure 2. As it can be seen, the increase d quality of care and service has the highest percentage of participants according to the statistics. On the other hand, model with predictive analysis has the lowest level of participants.

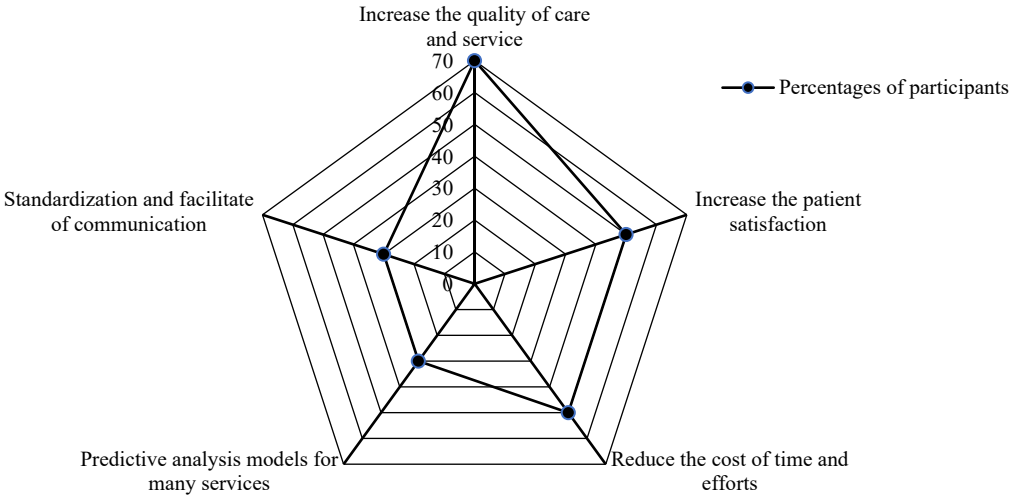

Figure 2. Benefits of IoT technologies for patients [11]

3.3. Ambient Assisted Living (AAL) Healthcare

The goal of using AAL in a home setting is to provide a service related to unconscious healthcare. AAL offers health management and actively seeks to age via the use of ICT on a two-way platform that is monitored in real-time from both directions. As part of the user's normal routine, they may get health information automatically, track their health condition, adopt good behaviors, and enhance their diet and activity levels. As stated by Choi, et al. [12], its main goals are to automatically retrieve users' health records and to help them correct unhealthy behaviors and posture via constant monitoring. Figure 3 shows how the platform's data will be utilized as big data by affiliated local societies and professional medical organizations to deliver reliable information to healthcare service providers. As it can be seen, the AAL system is a combination of healthcare and architecture with IoT ensures multi-dimensional data collection and make an interconnected relation among them. The system ensures a reliable data collection and feedback platform for elderly people.

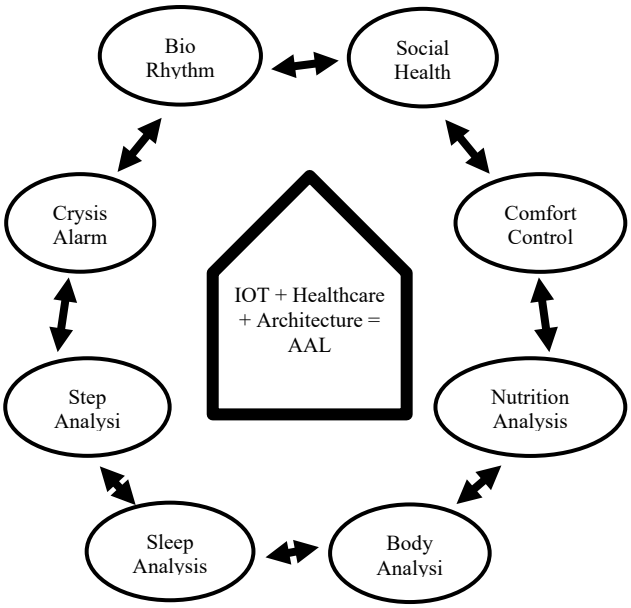

Figure 3. Typical layout of the AAL healthcare system [12]

In terms of resident/device interaction and device longevity, sensors, screens, and other electronic devices used in AAL healthcare services fall in between typical electronic equipment and architectural infrastructure. Hence, it is crucial to govern the installation of devices and ensure they are put on the architectural framework to facilitate easy replacement. study is now underway to develop an installation system for AAL healthcare services using ceiling and wall mounts.

3.4. WSN Based SHHS Technology

Wireless sensor networks (WSNs) have been a game-changer and ubiquitous trend across all industries; they are a key component of internet of things (IoT) solutions and systems that enable the connection of numerous autonomous sensors in different locations to a shared network for the purpose of data exchange and transmission. For example, WBANs -wireless body area sensor networks- are able to calculate and transmit physical features and parameters; as a result, they are implanted or connected inside the human body or positioned in a particular location for use in healthcare [13]. In general, Smart home healthcare systems based on Wireless Sensor Networks (WSN-SHHS) hold the capability to incorporate compact, low-power, intelligent medical sensor devices seamlessly into the existing electronic infrastructure of patients' homes. This integration introduces a genuinely ambient intelligent element into our daily lives.

4. BARRIERS IN SHHS

4.1. Security Issues in SHHS

4.1.1. Data Privacy (Unauthorized Access)

Smart home healthcare systems often collect and store sensitive health data. Unauthorized access to this data can lead to privacy breaches and misuse of personal information. A systemic review suggests that the three primary impediments to adopting Smart Home Technology (SHT) are privacy, security, and hacking concerns (80.65%); technical reliability, warranties, and obsolescence (80.65%); and issues related to usability, user acceptance, and learning (77.42%). According to various survey outcomes, 79.7% of respondents express apprehension regarding privacy and security regulations.

The findings reveal that 78.8% of participants harbor anxieties about utilizing smart home devices to access private data and monitor user behavior. Public awareness and functionality levels are persistently at the forefront of users' concerns. In general, user privacy emerges as a significant worry, stemming from their perceived inability to control personal and private information. These concerns are measured to heighten user awareness of invasion risks, ultimately working towards minimizing privacy-related issues.

4.1.2. Device Security (Vulnerabilities in Devices)

Smart healthcare devices may have security vulnerabilities that could be exploited by malicious actors. Regular software updates and security patches are essential to address these vulnerabilities. Users sometimes neglect to change default usernames and passwords on smart devices, making them susceptible to hacking. When it comes to smart or connected health, communication is a big obstacle. Nowadays, a lot of gadgets are equipped with sensors that may gather data, and they often connect to the server in their native language. Because every manufacturer has their own secret protocol, it's not always possible for sensors from various brands communicate to one other. Hence, it's crucial to test medical equipment with different wireless communication methods to ensure they work effectively when linked. In order to withstand any security breaches, smart healthcare systems need to be ready to deal with any dangers that may arise. Akmandor and Jha [14] stated that, treatment decisions, and growing alarms is essential to produce a good choice maker on image retrieval at crucial phases.

4.1.3. Network Security (Insecure Networks and Man-in-the-Middle Attacks)

The reliance on home networks introduces the risk of unauthorized access if the network is not properly secured. Implementing strong Wi-Fi encryption, such as WPA3, and securing routers with unique passwords are essential measures. Attacks where a third-party intercepts communication between devices and the central healthcare system can compromise the integrity and confidentiality of data. By using a man-in-the-middle attack, cloud polling redirects traffic in order to inject commands directly into a device. A man-in-the-middle attack requires some kind of communication connection. According to Mallik [15] the most common methods of man-in-the-middle attacks on communication networks are GSM, UMTS, LTE, Bluetooth, NFC, Wi-Fi, and Radio Frequency. Hackers may breach an IoT system using the MitM concept by changing the traffic flow, reconfiguring the network architecture, creating fake identities, and generating harmful and misleading information. These are some of the varieties of MitM attacks: eavesdropping, Sybil, Wormhole, Identity replication, Node replication, and so on.

4.1.4. Cloud Data Storage and Transfer Security

Storing patient healthcare information on a cloud server is a frequent practice. The biggest concern is the possibility that third parties may access and use patients' medical records, as the healthcare business heavily relies on public cloud services. Securely transmitting data from smart devices to the cloud is crucial. Negligible healthcare services and sensitive patient data might result from malicious individuals abusing vulnerabilities in the Cloud IoT network. When Cloud and IoT are combined, the situation will get much worse, and hidden weaknesses and difficulties will be revealed. Cloud IoT networks include billions of linked nodes that might be exploited by malicious actors due to security issues. So, even if the Cloud IoT network has many advantages, its flaws will make them irrelevant. Also, due to the financial consequences, replacing deployed sensor nodes on a regular basis is not feasible. In order to function for long periods of time without replacement or maintenance, the core security architecture must be strong and resilient.

4.1.5. Authentication and Device Tampering

The enormous number and sophistication of newly discovered software and hardware security flaws makes it difficult to quickly identify possible threats. As more and more gadgets are being linked to the Internet, this problem is only becoming worse. The attack surface is already high due to the use of default authentication and the prevalence of unsecured Web-based interface access. In order to rapidly and securely authenticate distant end-users on behalf of medical sensors, Moosavi, et al. [16] suggested a secured and efficient authentication (SEA) architecture that makes use of distributed smart e-health gateways. Essentially, a gateway's primary function is to facilitate communication between devices and various wireless protocols.

On the other hand, most smart home devices are physically accessible, which makes them vulnerable to assaults that involve physical manipulation. As an example, homeowners might sometimes launch this assault by interfering with smart meters in an effort to lower their billing expenses. Aside from malicious individuals, other entities might also use technological manipulation to make it easier to break in.

4.1.6. Denial of Service Attack (DoS)

The goal of a DoS attack is to prevent other nodes from accessing resources by flooding the system's data transfer with unknown traffic. This prevents other nodes from sending their information because they detect that the channel is busy. An attacker often uses NAV behavior by tempering a part of the flags in control frames in a DoS attack. Detecting this kind of attack is challenging in the IEEE 802.11 standard because nodes do not counter-check all of the flags in control packets. Without proper identification and authorization, a DoS assault might compromise patient data. Additionally, a DoS attack will block all data from reaching any of the network's sensors by flooding the system's data channel.

The availability of systems or healthcare services, the efficiency of networks, and the responsibility of sensors are all compromised by this kind of assault. An adversary may inject fake information about a patient, send out misleading information about a patient, or even add bogus information about a patient in a DoS attack. They can even repeat previous messages to make them seem current. A denial-of-service attack may manifest in a variety of ways and often targets a specific layer of the network.

4.1.7. Interoperability and Regulatory Compliance

Failure to Comply with Regulations: Smart home healthcare services must comply with healthcare regulations and data protection laws. The capacity for devices and services to communicate with one another and with other IoT domains is essential for users and service providers. Because of the wide variety of regulatory bodies that oversee the many fields included by the IoT, this presents complicated problems. Medical standards need strict controls, which further complicates situations in linked health circumstances. As stated by Firouzi, et al. [17] before developing smart health apps for the healthcare industry, companies should research and understand the rules and regulations set forth by the adjacent administrations.

4.2. Security Concern in the Context of Saudi Arabia

In Saudi Arabia, it is thought that people are becoming more aware of the use of SHT devices, but security and privacy concerns are also rising. The devices can now collect significant volumes of data and deliver sensitive and personal information that can sometimes lead to customer threats and privacy issues. Moreover, such concerns are not only related to the possible mishandling of sensitive information, but Consumers express apprehension about managing and safeguarding their data. According to survey findings, 79.7% of respondents are

uneasy about privacy and security regulations. The results indicate that 78.8% of participants harbor concerns about utilizing smart home devices for accessing private data and monitoring user activities.

The predominant focus for many users continues to be the limited awareness and functionality of such devices. Overall, user privacy emerges as a primary concern, with worries stemming from the inability to control personal and private information. These concerns aim to raise awareness among users regarding potential privacy infringements, ultimately minimizing related issues. Despite some customers having confidence in the advantages of Smart Home Technology (SHT) services, with 80.7% expressing concerns about security vulnerabilities in smart home devices, including potential vendor attacks. This underscores the need for addressing security risks even when users perceive the benefits of SHT services positively.

5. BLOCKCHAIN TECHNOLOGY IN SHHS

5.1. Significance of Blockchain in Resolving Security Issues

Despite an increasing number of studies investigating blockchain's usefulness in other fields, the healthcare industry is falling behind. There are a lot of factors contributing to this. One important cause is the critical scarcity of blockchain professionals with expertise in the healthcare industry. An innovative and smart healthcare system is replacing the old, inefficient ways of healthcare in the sector. As it navigates this period of transformation, the healthcare industry faces a multitude of impending problems. Many risks, such as data theft, compromised security and privacy, ownership control, etc., affect modern smart healthcare systems. With the use of blockchain technology, advanced medical treatments may be delivered in a more private and protected way. Many of the problems that contemporary smart healthcare systems are experiencing may be solved with the use of blockchain technology and its many advantages. As stated by many authors, blockchain technology has become an essential component of healthcare research because to its distributed ledger, decentralized storage, authentication, security, and immutability.

However, no patient identification has emerged as the gold standard despite extensive study in the healthcare industry. It might lead to electronic health records not matching. To get around this problem, we may move patient data to the blockchain, where it will generate a unique hashID value for each patient [18]. It is possible to identify a patient using this hashID without disclosing his actual identity. In this way, both data openness and patient privacy are protected. The fact that the whole record belongs to the blockchain rather than any one hospital or other medical institution helps to settle data ownership disputes as well. Unreasonable restrictions on the transfer of patients' electronic health records may be detected and removed using this function. By dispersing all of the patient data, the distributed ledger technology known as blockchain eliminates the potential of a central point of failure. By requiring the execution of a consensus mechanism for the addition of any block to the current blockchain, conventional database systems eliminate the risk of human mistake when inputting data. Insurance firms, pharmaceutical corporations, the healthcare supply chain, and others in the healthcare industry also benefit from blockchain technology.

According to Yli-Huumo, et al. [19] the basic technologies in a blockchain-based smart healthcare system are largely identical to those in a traditional system, with the addition of the blockchain idea to manage the confidentiality and integrity of patient records and information. In contrast to centralized cloud storage and monitoring, blockchain offers, depending on the blockchain type, a distributed and decentralized method of data storage. The addition of this functionality ensures data openness while protecting the privacy of the patient's personal and medical information. With the patient serving as the principal delegator and the blockchain using the idea of smart contracts, the permission and access to data may be effectively controlled. The permanence feature is added to the personal and medical data since once a transaction is logged, it cannot be hacked. Information recorded in a blockchain will be accessible for researchers to access in the future. Additionally, it makes it easier to trace and monitor the movement of pharmaceuticals and other healthcare items along the supply chain. It is simpler to audit and ensure compliance using blockchain because to its immutable nature. The healthcare industry stands to benefit greatly from blockchain technology because of its distinct characteristics.

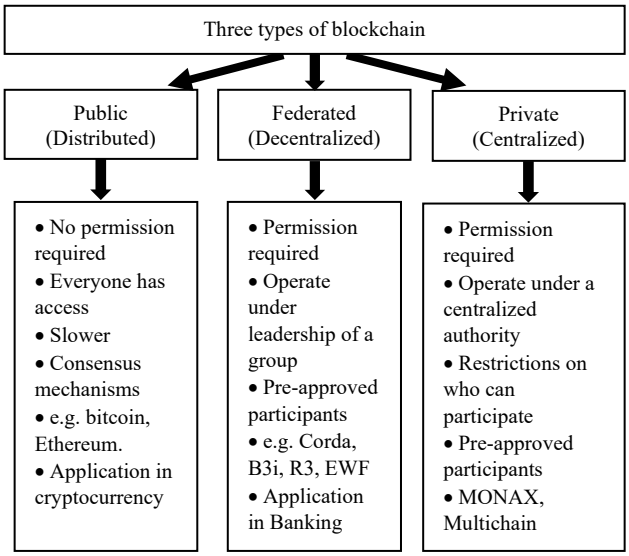

Figure 4. Different types of blockchain technology [18]

Figure 4 depicted different types of blockchain architecture used in healthcare and other IT field. As it can be seen public blockchains, like Bitcoin and Ethereum, are open to anyone and rely on a decentralized network of nodes to validate and record transactions, ensuring transparency and immutability. Federated blockchains involve a group of organizations working together, each maintaining a node and sharing control over the network.

This approach enhances scalability and efficiency while retaining a degree of decentralization. In contrast, private blockchains are restricted to a specific group or organization, providing more control over access, permissions, and data privacy. Private blockchains are suitable for applications where participants are known and trusted, allowing for greater efficiency and faster transaction processing.

5.2. Multi-Layer Blockchain for Smart Health Framework

Albahli, et al. [20] has put up a model that takes into account the following situations: To begin, in order to establish an EHR, the patient needs to gather data from chains and nodes. Then, access to electronic health records has been granted to the patient or practitioner. Further blocks may then be added by the patient as a result of his medical visit, as seen in Figure 5. The framework developed by Albahli, et al. [20] has five distinct tiers. The suggested framework might decrease the cost of safeguarding and preserving patients' information by storing and sharing seamless health data across multiple organizations using blockchain technology and the cloud computing supplied by. Furthermore, in order to keep EHRs immutable, patient privacy and healthcare domain security are safeguarded. As a result, improving performance with cryptography adoption to safeguard medical data is possible by merging blockchain with the technique of. As an integral aspect of the blockchain technology, the suggested architecture also provides unchangeable medical records.

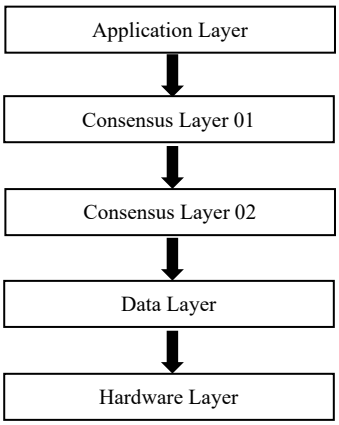

Figure 5. Blockchain technology for patient medical records [20]

5.3. Advantages of Blockchain Technology in the Field of SHHS

As it offers perfect application cases in a variety of technical and social fields, blockchain technology is gradually being hailed as a boon of contemporary computing. In terms of potential for growth and development, the healthcare sector is like an economy on a roller coaster. Applying blockchain technology to the healthcare sector has several advantages, both immediate and long-term. Here are a few examples:

- Medical and clinical data of patients stored in a distributed and secure manner.
- Launch the Patient-Centric Network.
- Clear Procedures for Audit Trials.
- Facility and service monitoring and holistic quality management.
- Supply chain management that is both secure and transparent.
- Control and management system that is both trustworthy and unchangeable.
- Facilitates the discussion and exchange of information via patient mediation.
- Information is secured by using immutable blocks that are organized in a chain-like pattern.
- Encourage more patient participation at all stages of care, from diagnosis to treatment and finally to recovery.
- Eliminate reliance on a central node (everyone has the same rights and privileges).

6. PROPOSED BLOCKCHAIN FRAMEWORK

The foundation of the whole proposed system is the integration of IoT, Blockchain, and Machine Learning for detecting abnormalities in the patient's health data's behavior [21]. The presented approach is essentially a system that requires the patient's wearable gadgets to transmit data, and the IoT module is used to intercept and retrieve this data. Patients' information is best stored and maintained using the shown blockchain system, which allows for many transactions and supports access management for various stakeholders. The pseudo-anonymity of patient identification and the provision of verified and trustworthy data are two further ways in which the Blockchain architecture supports medical research, allowing for more precise findings. Fig. 8. Depicted the systematic framework Formulated to address current concerns regarding security and privacy. The whole framework is a combination of three module:

6.1. The IoT Module

Data acquisition and processing from biosensors and wearable devices, whether such devices are on the patient or in their surrounding environment, is the focus of this module [22]. More obviously, the optimal method for monitoring a patient's continuous data, especially during a gentle therapy followed by medical testing, is through the use of a wearable sensor. The wearable device can gather a range of information including heart rate, calorie expenditure, respiratory strength, and sleep stages, providing comprehensive insights into the patient's physiological responses every second.

6.2. Blockchain-Based Access and Transaction Control

Two critical blockchain networks, the Personal Health Care (PHC) Blockchain and the External Record Management (ERM) Blockchain, have been explicitly outlined in the proposed design [21]. It is common practice for patients to be the ones to manage their own personal healthcare blockchain, which collects data from various wearable devices. By providing the doctor with access to the data, we can help them better comprehend the patient's condition and prescribe the right prescription. External to the wearable devices, the blockchain network governs the storage of data in a cloud database.

The data created during a patient's visit to the doctor is managed using the External Record Management Blockchain. Data often stored on the ERM Blockchain includes information from medical facilities, medications, images, medical test results, pharmacy costs, and medical institutions themselves. It is the "Proof of Stake" method that ensures data is only added to the chain when all blockchain stakeholders agree on it [21]. Since all other stakeholders in ERM Blockchain are effectively a combination of the Healthcare Center and the Doctor, they possess the bulk of the stakes.

6.3. Machine Learning Module

In order to identify any kind of abnormality, the Machine Learning Module uses the data that the patient has provided. Running the model to retrieve irregularities in the produced data may greatly address the anomaly detection. The doctor is notified if an abnormality is found, and appropriate action may be taken depending on the situation [21].

6.4. Performance Comparison of Proposed Framework

The adoption of our proposed blockchain-based smart healthcare system represents a paradigm shift in the realm of security and privacy compared to traditional healthcare models. The decentralized and cryptographic nature of blockchain in this framework ensures a heightened level of security for sensitive patient data. By employing advanced encryption techniques in this system, blockchain mitigates the risks associated with unauthorized access, data breaches, and tampering, safeguarding patient information throughout its lifecycle. The elimination of a central authority in favor of a distributed ledger enhances privacy, reducing the vulnerability to single points of failure. Smart contracts, inherent to blockchain, facilitate secure and automated execution of healthcare processes, minimizing the exposure of personal data and preventing unauthorized handling.

Moreover, the transparent and auditable nature of this blockchain transactions instills trust among stakeholders, as patients, healthcare providers, and insurers can trace and verify every interaction with the system. In summary, the blockchain-based smart healthcare system proposed in this study not only fortifies security mechanisms but also establishes a robust foundation for preserving patient privacy in the digital age. Several similar type of healthcare system can be seen in the field of sensor and cloud-based healthcare platform. Through the use of information and communication technologies (ICT) on a bidirectional platform that is monitored in real-time from both sides, AAL provides health management and actively aims to age. Integrating health information, tracking one's condition, adopting healthy habits, and improving one's diet and exercise levels into one's regular routine are all possible. Nevertheless, several researchers have found security and privacy flaws in the system. If that's the case, reducing the impact of such dangers may be achieved by using proposed blockchain framework.

7. OTHER NON-SECURITY ISSUES

The accuracy of sensors and devices used in smart healthcare applications is crucial for making reliable health-related decisions. Calibration and regular maintenance are essential. Dependence on network connectivity may introduce issues in areas with poor internet or during network outages, affecting the real-time monitoring capabilities of smart home healthcare systems. The design of user interfaces should be user-friendly and accessible, especially for older adults or individuals with limited technical proficiency. Some individuals may resist adopting smart home healthcare services due to concerns about technology, privacy, or a preference for traditional healthcare methods.

As the number of users and devices increases, the infrastructure supporting smart home healthcare services must be scalable to accommodate the growing demand without compromising performance. The cost of implementing and maintaining smart home healthcare systems can be a barrier to widespread adoption. It is imperative that all socioeconomic groups be able to purchase WMD equipment. Consideration of cost-effectiveness need to be made throughout the design stage. Wearable devices may be made more affordable with the use of Flexible Hybrid Electronics (FHE) [23]. Flexible electronics and silicon technologies are combined in it.

8. IMPLEMENTATION OF SHHS

8.1. Implementation of SHHS by Electronic Health Record and AI

The Saudi Healthcare Council (SHC) is a regulatory agency that monitors the Saudi healthcare industry and supports the use of technology in healthcare. SHC further illustrates the government's dedication to encouraging the use of SHS and eHealth. Also, the Saudi Arabian Ministry of Health (MoH) has made great efforts recently to adopt digital transformation and improve its healthcare services. For instance, Saudi Arabian MoH initiated a number of digital transformation initiatives in 2016 to modernize and simplify its healthcare services [24]. These initiatives covered a range of healthcare system components, including Electronic Health Records (EHRs), telemedicine, and the development of smart healthcare facilities across Saudi Arabia.

The MoH's adoption of an advanced EHR mechanism across Saudi Arabia's medical institutions was one of its major priorities. EHR adoption has been acknowledged as a crucial step towards improving patient outcomes and the effectiveness of healthcare delivery. The growth of telemedicine services was another key MoH initiative. Telemedicine facilitates virtual health consultations, diagnoses, and treatments, rendering accessible medical services to patients residing in remote areas in Saudi Arabia. The MoH's focus on telemedicine aligns with its mission to improve patient satisfaction and healthcare accessible, particularly for underprivileged communities. The MoH has also concentrated on building smart healthcare facilities using cutting-edge technology. These facilities are made to improve patient experience, make the most use of available resources, and use data analytics to make wise decisions.

The use of EHRs with telemedicine services can result in more effective diagnosis and treatment by eliminating medical mistakes and enhancing complete care quality. Also, incorporating sophisticated analytics and artificial intelligence (AI) in healthcare operations has led to the development of reliable technology infrastructures. Additionally, the Saudi Arabia MoH's initiatives for digital transformation have the potential to draw investments, partnerships, and collaborations from leading technology and healthcare businesses. Saudi Arabia can promote information sharing, technology transfer, and innovation in the healthcare industry by portraying itself as a leader in the field, which will be advantageous to both the local populace and the international healthcare community.

In the context of Saudi Arabian healthcare system our proposed blockchain framework can enhances the security and integrity of health data by ensuring tamper-resistant and immutable record-keeping. Its decentralized and shared ledger facilitates interoperability among healthcare providers, fostering seamless data exchange. Patient-controlled access and consent management are streamlined through smart contracts, granting individuals greater control over their health information [21]. In AI, blockchain enables secure and privacy-preserving data sharing for model training, supporting advancements in healthcare analytics.

8.2. Healthcare Apps in SHHS Implementation

The COVID-19 pandemic has brought about unprecedented challenges to medical mechanisms globally, including in Saudi Arabia [25]. Multiple healthcare applications have been released in reaction to the issue to help and support both healthcare professionals and the general public. Healthcare apps have been valuable for COVID-19 experimenting, consulting, and contact tracing. For example, the "Tawakkalna" app launched by the Saudi Arabian MoH has emerged as a primary mechanism in the nation's initiatives to control the spread of COVID-19 [26]. The app enables users to obtain their COVID-19 status, schedule vaccination timing with doctors, and generate travel permits during lockdowns. It has been crucial in simplifying procedures and guaranteeing adherence to public health regulations.

In addition, Saudi MoH's "Mawid" app allows patients to schedule visitations, check medical records, and remotely enhance consultations with medical experts. This guarantees continuity of care and lightens the load on medical institutions so they may concentrate on urgent situations. Users of these applications may get the most recent information on the pandemic, precautions, and health officials' recommendations. The Saudi Ministry of Health created the "Sehha" app as a comprehensive source of COVID-19 knowledge to assist people in staying informed and making wise decisions. These apps have enabled access to healthcare and improved the control of virus transmission through effective screening, tracking, and information distribution.

However, mobile apps can leverage blockchain for tokenized payments, supply chain traceability, decentralized identity solutions, and real-time data synchronization. While offering enhanced security and transparency, the implementation of blockchain in mobile apps requires careful consideration of factors like scalability and user experience to fully capitalize on its potential. The Saudi Arabian health industry can consider those facts to successfully implement blockchain based secure mobile app healthcare network. The MoH in Saudi Arabia has made tremendous strides in digital health by introducing a number of applications to improve healthcare infrastructure and ease the increasing demands for basic healthcare services. The MoH's creation of the 973 number for remote medical assistance is one noteworthy move. This service eliminates the necessity for in-person visits to healthcare facilities by allowing people to get medical advice and consultation online.

The Sahaty and Sehah applications have also proven crucial in offering virtual health consultations and support. With the use of these apps, people may consult healthcare experts remotely, get advice from doctors, and get support for a range of health issues. The Mawoad app, which the MoH also released, allows people to make appointments before attending healthcare facilities. This project attempts to maximize the use of healthcare resources by streamlining the patient experience and cutting down on wait times. The Saudi Arabian MoH has greatly improved the general patient experience by utilizing technology to make scheduling appointments easier. However, Figure 6 illustrates the WSN based cloud smart healthcare system which can be implemented using a combination of mobile apps and wireless sensors.

8.3. Challenges to SHHS System Adaptation

There are many factors that contribute to the low adoption rate, including privacy and security concerns, lack of trust in technology, perceived risk, lack of awareness and education, and the complexity of the technology. In the first place, there are anxieties about patients' privacy and security in Saudi Arabia. This is because patients are cautious about sharing their personal health data with healthcare experts in Saudi Arabia, which hampers the SHHS adoption rate in the country. One of the primary factors for the low adoption of SHHS in Saudi Arabia is privacy and security anxieties. Patients are reluctant to share their personal health information with healthcare professionals because of fears of data breaches or misuse in Saudi Arabia. According to many scholars, privacy and security apprehensions are among the primary hurdles to the low adoption of e-health services in Saudi Arabia. The research discovered that patients are anxious about the privacy of their private health data and the likelihood of it being retrieved by unauthorized private.

However, implementing a blockchain-based smart healthcare system presents several technical challenges [27]. Scalability is a primary concern, as the growing volume of healthcare data may strain the network's capacity. Interoperability with existing healthcare systems and standards is another hurdle, requiring seamless integration to ensure data flow across diverse platforms. Privacy concerns demand robust solutions for handling sensitive patient information securely. Additionally, smart contract vulnerabilities and the need for standardized protocols further complicate implementation.

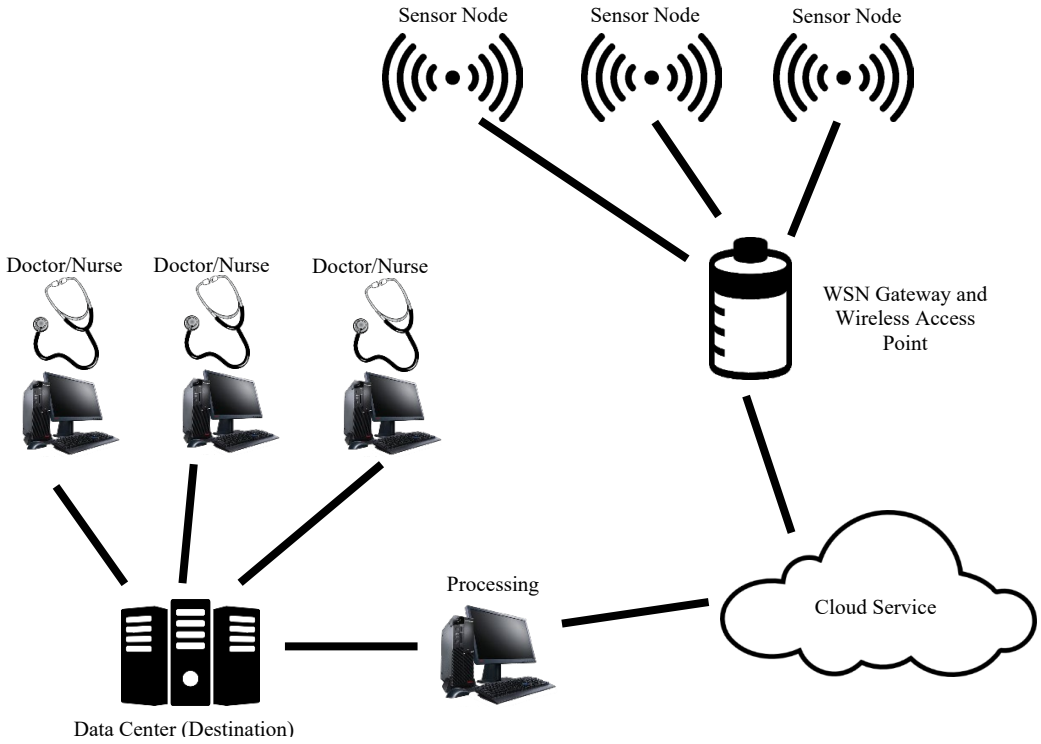

Figure 6. A WSN based healthcare network which can be implemented using mobile apps [13]

9. FUTURE RECOMMENDATION

The advancement of infrastructure and connectivity is crucial for the future of blockchain technology in healthcare, as it will facilitate its simple implementation. It is also necessary to address problems with scalability, network congestion, and the broad use of blockchain systems. Stakeholders' lack of knowledge is a big obstacle to blockchain adoption that will need future attention. The use of blockchain technology has increased exponentially across all industries since its launch in 2008. While research into blockchain's healthcare applications is in its infancy, the technology shows enormous promise for revolutionizing the industry.

10. CONCLUSIONS

Based on the extensive review we can conclude that, SHHS can enhance healthcare results, as patients can receive continuous tracking and early discovery of any healthiness abnormalities. SHHS's virtual supervision of patients with chronic illnesses such as diabetes, heart failure, and chronic obstructive pulmonary disease (COPD) could improve patients' well-being. There are a number of obstacles that must be overcome before digital health care can become commonplace, despite the growing interest in using IoT and big data technology to improve efficiency in the health-care industry. The biggest challenge, apart from the broad implementation of SHHS in Saudi Arabia is privacy and security, which includes problems like data privacy, unauthorized access, cloud data and transfer security etc. However, combining blockchain with other cutting-edge technologies has the potential to revolutionize smart healthcare systems, taking them from insecure and centralized to distributed and decentralized, all while enhancing the quality of medical and related services. There are a number of reasons to think at blockchain technology as a way to enhance the healthcare system. One benefit is that it helps keep patients' personal information private while yet making it available to all parties involved. Second, the sensitive medical records are protected from any kind of data theft or eavesdropping, and it becomes very difficult for malevolent intruders to alter them. Finally, the proposed blockchain based structure discussed in this study can fully resolves the problem with the traditional healthcare system's data security and privacy while simultaneously increasing efficiency. From the very beginning to the very end, the suggested framework provides comprehensive monitoring of a cure, a continuous therapy, or generic healthcare.

REFERENCES

[1] M. Al Rawashdeh, P. Keikhosrokiani, B. Belaton, M. Alawida, A. Zwiri, "IoT Adoption and Application for Smart Healthcare: A Systematic Review", Sensors, Vol. 22, No. 14, p. 5377, 2022.

[2] M.A. Khan, M.T. Quasim, F. Algarni, A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia", The 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), IEEE, pp. 1-5, 2020.

[3] G. Mouhcine, T. Jonas, W. Catherine, E. Khalil, "Context-Based Access Control to Medical Data in Smart Homes", International Conference on Computer Engineering and Applications (IPCSIT'2011), Vol. 2, pp. 275-279, 2011.

[4] M.I. Pramanik, R.Y. Lau, M.A.K. Azad, M.S. Hossain, M.K.H. Chowdhury, B. Karmaker, "Healthcare Informatics and Analytics in Big Data", Expert Systems with Applications, Vol. 152, p. 113388, 2020.
[5] A. Kichloo, et al., "Telemedicine, the Current COVID-19 Pandemic and the Future: A Narrative Review and Perspectives Moving Forward in the USA", Family Medicine and Community Health, Vol. 8, No. 3, 2020.
[6] S. Kumar, H. Kumar, "LUNGCOV: A Diagnostic Framework Using Machine Learning and Imaging Modality", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 190-199, June 2022.
[7] J.M. Bingham, et al., "Impact of Telehealth Interventions on Medication Adherence for Patients with Type 2 Diabetes, Hypertension, and/or Dyslipidemia: A Systematic Review", Annals of Pharmacotherapy, Vol. 55, No. 5, pp. 637-649, 2021.
[8] W.M.G. Alshammari, F.M.M. Alshammari, F.M.M. Alshammry, "Factors Influencing the Adoption of E-Health Management among Saudi Citizens with Moderating Role of E-Health Literacy", Information Management and Business Review, Vol. 13, No. 3(I), pp. 47-61, 2021.
[9] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing", IEEE Access, Vol. 7, pp. 74361-74382, 2019.
[10] G.A.f. Statistics, "General Authority for Statistics Saudi Arabia" October 2023, www.stats.gov.sa/en.
[11] J. Bugeja, A. Jacobsson, P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes", The 2016 European Intelligence and Security Informatics Conference (EISIC), IEEE, pp. 172-175, 2016.
[12] D. Choi, H. Choi, D. Shon, "Future Changes to Smart Home Based on AAL Healthcare Service", Journal of Asian Architecture and Building Engineering, Vol. 18, No. 3, pp. 190-199, 2019.
[13] A. Onasanya, S. Lakkis, M. Elshakankiri, "Implementing IoT/WSN Based Smart Saskatchewan Healthcare System", Wireless Networks, Vol. 25, pp. 3999-4020, 2019.
[14] A.O. Akmandor, N.K. Jha, "Keep the Stress Away with SoDA: Stress Detection and Alleviation System", IEEE Transactions on Multi-Scale Computing Systems, Vol. 3, No. 4, pp. 269-282, 2017.
[15] A. Mallik, "Man-in-the-Middle-Attack: Understanding in Simple Words", Cyberspace: Journal of Information Technology Education, Vol. 2, No. 2, pp. 109-134, Indonesia, January 2019.
[16] S.R. Moosavi, et al., "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways", Procedia Computer Science, Vol. 52, pp. 452-459, 2015.
[17] F. Firouzi, B. Farahani, M. Ibrahim, K. Chakrabarty, "Keynote Paper: from EDA to IoT eHealth: Promises, Challenges, and Solutions", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 37, No. 12, pp. 2965-2978, 2018.
[18] G. Tripathi, M.A. Ahad, S. Paiva, "S2HS-A Blockchain Based Approach for Smart Healthcare System", Elsevier, Healthcare, Vol. 8, No. 1, p. 100391, 2020.
[19] J. Yli Huumo, D. Ko, S. Choi, S. Park, K. Smolander, "Where is Current Research on Blockchain Technology? A Systematic Review", PloS One, Vol. 11, No. 10, p. e0163477, 2016.
[20] S. Albahli, R.U. Khan, A.M. Qamar, "A Blockchain-Based Architecture for Smart Healthcare System: A Case Study of Saudi Arabia", Adv. Sci. Technol. Eng. Syst, Vol. 5, No. 1, pp. 40-47, 2020.
[21] S. Chakraborty, S. Aich, H.C. Kim, "A Secure Healthcare System Design Framework Using Blockchain Technology", The 21st International Conference on Advanced Communication Technology (ICACT), IEEE, pp. 260-264, 2019.
[22] M.N. Al Otaibi, "Internet of Things (IoT) Saudi Arabia Healthcare Systems: State-of-the-art, Future Opportunities and Open Challenges", Journal of Health Informatics in Developing Countries, Vol. 13, No. 1, 2019.
[23] U. Gupta, J. Park, H. Joshi, U.Y. Ogras, "Flexibility-Aware System-on-Polymer (SoP): Concept to Prototype", IEEE Transactions on Multi-Scale Computing Systems, Vol. 3, No. 1, pp. 36-49, 2016.
[24] B. Binhadyan, K. Peszynski, N. Wickramasinghe, "Using e-Mental Health Services for the Benefit of Consumers in Saudi Arabia", Contemporary Consumer Health Informatics, pp. 367-377, 2016.
[25] A. Odeh, M. Odeh, "Increasing the Efficiency of Online Healthcare Services Software and Mobile Applications using Artificial Intelligence Technology", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 44, Vol. 12, No. 3, pp. 16-22, September 2020.
[26] M. Hassounah, H. Raheel, M. Alhefzi, "Digital Response During the COVID-19 Pandemic in Saudi Arabia", Journal of Medical Internet Research, Vol. 22, No. 9, p. e19338, 2020.
[27] M.H.R. Sobuz, et al., "Assessment of Mechanical Properties with Machine Learning Modeling and Durability, and Microstructural Characteristics of a Biochar-Cement Mortar Composite", Construction and Building Materials, Vol. 411, p. 134281, 2024.

BIOGRAPHIES

Name: **Omar**
Middle Name: **Mutheeb**
Surname: **Almutairi**
Birthday: 28.10.1984
Birthplace: Riyadh, Saudi Arabia
Bachelor: Computer Science, Umm Alqura University, Mecca, Saudi Arabia, 2007
Master: IT Advanced, Queensland University of Technology, Brisbane, Queensland, Australia, 2016
Doctorate: Student, Department of Computer Science, Science University of Malaysia, Penang, Malaysia, Since 2021

The Last Scientific Position: Lecturer, Computer Science, Shaqra University, Shaqra, Saudi Arabia, Since 2013
Research Interests: Internet of Things, Healthcare Technologies, CyberSecurity
Scientific Publications: 1 Paper

Name: **Mohd Najwadi**
Surname: **Yusoff**
Birthday: 03.06.1987
Birthplace: Penang, Malaysia
Bachelor: ICT, Petronas University of Technology, Perak, Malaysia, 2009
Master: Master of Science, Computer Science, Science University of Malaysia, Penang, Malaysia, 2011
Doctorate: Security in Computing, University of Putra Malaysia, Serdang, Selangor, Malaysia, 2016
The Last Scientific Position: Senior Lecturer, Computer Science, Science University of Malaysia, Penang, Malaysia, Since 2013
Research Interests: Cyber Security, Cyber Threat Intelligence (AI), Blockchain, Quantum Cryptography, Software Vulnerabilities
Scientific Publications: 8 Papers
Scientific Membership: Malaysia Board of Technologists (MBOT)

Name: **Adel**
Middle Name: **Aboud**
Surname: **Bahaddad**
Birthday: 01.07.1976
Birthplace: Jeddah, Saudi Arabia
Bachelor: Computer Science, King Abdul Aziz University, Jeddah, Saudi Arabia, 2002
Master: IT, Griffith University, South East Queensland, Australia, 2011
Doctorate: School of IT, Griffith University, South East Queensland, Australia, 2017
The Last Scientific Position: Assist. Prof., Computer Science, King Abdul Aziz University, Jeddah, Saudi Arabia, Since 2008
Research Interests: Technology Adoption, Internet of Things, Healthcare Technologies, CyberSecurity
Scientific Publications: 9 Papers