International Journal of Computational Intelligence in Control

Security and Privacy Issues in Challenging World of Medical Technology

Mudasir Mahmood[1]*,Muhammad Ijaz Khan[1], Ziauddin[1], Fareedullah[1], Syed Muhammad Ali Shah[1]
mudasir@gu.edu.pk, ijazkhan@gu.edu.pk, Ziasahib@gmail.com , fareedkamran44@yahoo.com , dikhan1112@gmail.com
[1]*Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan 29050*
[1]Corresponding Author: mudasir@gu.edu.pk : ijazkhan@gu.edu.pk

Abstract- ***The integration of new technology into the current infrastructure is transforming the face of medical healthcare. Currently, sensor networks for a patient in homes, shopping malls, parks, offices and in traveling monitor and electronic patient records are at the forefront of technology. Electronic versions of paper-based patient records are being created so that patients can access them online. The installation of specialized sensors inside the above mention places has made remote patient monitoring more feasible. By personalizing it and lowering expenses and medical blunders, the standard of medical care is raised by the combination of these technologies. Technology has many advantages that make the system socially acceptable, it is necessary to examine the Security& Privacy (S &P) concerns that go along with them. In this paper, we examine how these medical technologies may affect (S &P). We outline current problem-solving techniques and talk about which problem require more research.***

Keywords: Wireless sensor networks, Medical Healthcare systems, Security and Privacy

1. Introduction:

Long-standing issues in the medical care system includes the inability of doctors to easily obtain patient information, the inability of diagnoses to be written legibly on paper, and a lack of resources like (staff, time, and space) for patient monitoring. Opportunities exist to enhance the existing state of medical health through technological improvements in order to reduce some of these issues and offer more individualized medical care. For instance, the adoption of the Internet by medical health institutions over the past ten years has created a platform for the dissemination of general health information that enables people to learn more about their medical issues. Presently, over 90% of the roughly 5000 institutions that make up the American Hospital Association's membership reported having websites, with the majority of them featuring descriptive content about their facilities and services.

Today, a vast spectrum of technology is used in the medical sector. In this study, the adoption of Electronic Patient Records (EPR) as well as how the networks of sensors are used to monitor the patient online is discussed. As we know that many of the organizations are shifted to (EPRs), here the information is stored electronically instead of record in paper format and also enable the easy access and use. The American Medical Association (AMA), IEEE and other eight prominent nonprofit organizations in the fields of medicine and engineering came together to form “The Biotechnology Council”, an umbrella organization is assisting this transformation[1].

The main objective of the council is to standardize everything, including networking protocols and medical terminology allowing for the electronic storage and fast delivery of medical records anywhere in the world. While transferring the data in (EPRs), the small but rising number of medical health companies has created “Medical Health Websites” and “Web Portals" that provides customized patient services online [2]. See Table-1

Table-1: Best Medical Health Websites

S. No.	Best Medical Health Websites
1	Consumer & Patient Health Information Section (CAPHIS) | mlanet.org/caphis.
2	Center for Disease Control | cdc.gov.
3	healthline.com.
4	Mayo Clinic Health Information (MCHI)| mayoclinic.com/health-information.
5	mayoclinic.org.
6	medicalnewstoday.com.
7	Medline Plus | medlineplus.gov.
8	Merck Manuals | merckmanuals.com.
9	nih.gov.
10	PubMed Central | ncbi.nlm.nih.gov.
11	webmd.com.

The Common Functionality of Patient Portal Software is discussed as under: See Table -2

Table -2: Common Functionality of Patient Portal Software

Common Functionality of Patient Portal Software	
Appointment setting	Typically, patients can choose the most convenient time slot from a calendar that displays physician schedules in the portal. You can allow either live appointment scheduling or appointment requests, depending on your system. In the first scenario, patients ask for a certain time slot, the appointment will be confirm by the staff member in office and the patient will be informed later on. As the patient select the time slot while using online portal, there will be no need of staff involvement and a system will provide the live appointment schedule automatically by updating your practice management schedule.
Digital paperwork	The user is allowed to complete the important papers online instead of filling out the fresh patient registration forms by hand in the office. Office workers don't have to spend as much time scanning documents because the data is already digital. Patients can fill out satisfaction questionnaires and general health assessments on portals in addition to intake forms before or after a visit.
Medical records access	The importance of patient access to their own medical records cannot be overstated. These records provide a variety of information, such as clinical summaries, prescriptions, allergies, and more. Some practices are implementing the delivery of lab results exclusively online in order to encourage patients to use the program.
Online bill pay	The collecting method is done online with electronic billing statements. Through the patient portal, patients can securely pay their

	bills by debit or credit cards or by card number that is once submitted then the system will automatically handle all payments.
Prescription refills	By allowing patients to request refills through the portal, you may automate prescription renewal requests. The majority of systems offer a specific section where patients can enter their data (Medicine and Preferred Pharmacy) after that submit the request of prescription. The providers are then informed, and they use the portal to confirm, authorize, and/or handle the request.
Secure messaging	Instead of using the phone, communicate with patients via the portal, a secure electronic messaging platform is offered by most systems and send email to the patients whenever the care team communicates with them by sending a new message. The Provider response the messages that are send by the patient on portal.

These websites provide patients with access to their clinical laboratory results and other electronic patient data through a variety of customized services. Before, only doctors and other medical healthcare professionals had access to these services.

Another emerging technology is the sensor network. For remote patient monitoring, academic institutions as well as business are creating sensor systems. For instance, smart hospitals connect people, processes, and technologies to improve medical health globally. , The Integrated Digital Hospital (IDH) from Intel links people, processes, and technologies to improve medical health globally [3].

Smart hospitals seamlessly integrate technology to support the delivery of medical services in order to give the connected care that patients expect from leading institutions. As they incorporate new technologies to aid in patient care, hospitals in the modern era are going through a digital transition to fully enjoy the advantages of a connected, intelligent hospital, Integration is required throughout the hospital ecosystem and at all places where medical treatment is provided, from registration to imaging, the operating room to the nurses station. This is accurate despite the fact that many of the endpoint solutions used by hospitals to improve the accuracy and effectiveness of clinical procedures. By combining digital and physical resources into a unified framework that connects the institution's numerous clinical and business operations and assets, smart hospitals are comprehensively updating their infrastructure. Across the whole medical health ecosystem, including hospitals, clinics, providers, and beyond, smart hospitals have extensive data access enabling them to implement new life-saving innovations as they are produced. Additionally, they have sped up medical health processes and made patient trips easier. Using mobile point-of-care (MPOC) and other information technologies, the IDH system combines administrative and patient data to create a holistic, digital view of a patient's health. Assisted Living at Home Using Information Technology(ITALH) project at the University of California, Berkeley is looking into sensor networks for remote patient monitoring [4]. The objective of this project is to develop a wearable sensor-based system that will allow people who require assistance to remain in their own homes. Wide Area Body Networks (WABN) infrastructures are being developed through cooperation between Kansas State University and the University of Alabama in Huntsville [5].To monitor a patient's health while they are at home, shopping mall, parks, office or traveling the systems are being created Despite the fact that a number of (S & P) issues need to be looked into in order to advance and respect fundamental medical ethical principles and societal expectations, these technologies will significantly alter the way that medical care is delivered. Data access rights, data storage techniques and timeliness, data transmission security, data analysis rights, and governing policies are some of these issues. Even while medical data is now governed by laws, these laws need to be reviewed as new technology changes the way medical health is delivered. In this paper, the(S & P) concerns nearby patient monitoring through distant sensor networks and patient portals in electronic health records.

1.2. Sections:

This study is explained into different sections. Section 2 describes the background. The current regulatory framework for medical health data is presented in detail in Section 3, along with (S & P) worries about how the data will be utilized and shared in these systems. In order to improve system security and eliminate privacy problems, Section 4 looks at both existing solutions and what has to be done going forward. Section 5 wrap up with conclusion.

2. Background:

The technology employed by today's sensor networks for remote patient monitoring and EPRs include wireless connectivity and the Internet. We go into detail on the technological implementation of these platforms in order to stimulate conversation about (S & P) issues.

A. Electronic Patient Records (EPRs):

In order to make the current paper-based documentation available electronically, electronic patient records transform them to a digital version. The records contain a variety of information, including clinical lab results, MRIs, and doctor's comments. Health care records can be accessed instantly via EPRs, regardless of the user's location. The records are accessible online by patients, doctors, nurses, insurance companies, and patients themselves. EPRs lessen the frequency of mistakes caused by inconsistent and illegible word usage. In order to avoid data loss, backing up electronic documents is also easier than backing up physical records [6], [1].

The installation of EPRs includes a local database that gathers all the information for patient records in one location. For instance, a hospital might have its own electronic patient database. A clinician at one hospital can review patient data from another hospital by linking these local data bases across the Internet for data transmission. Using the Internet and interfaces created for presenting these records, such as the PCASSO and Vanderbilt patient portals, doctors, patients, and other medical healthcare professionals can all view a patient's information.

B. Monitoring of Patient Remotely at Home, Park, Office, and Shopping Mall and In Traveling:

Real-time patient monitoring in "at-home, park, office, shopping mall, and in transit" is now more feasible because to the development of sensor networks. Figure 1 depicts the whole setup for remote patient monitoring. The vital signs of a patient can be tracked by using a variety of sensors. In addition to conventional ambient temperature and humidity sensors, wearable gadgets like pulse oximeters and electrocardiogram sensors are also used. To perform various types of monitoring, new sensors are also being created. The Information Technology for Assisted Living at Home (ITALH)is creating, for instance, wearable fall detectors that use accelerometers [7]. Most of these systems use wireless communication, such as Zig Bee, Bluetooth, or other technologies, to transmit a periodic report from the sensors to a nearby base station. Data from the sensors is relayed back to a nearby base station, which could be a personal computer, for analysis. For instance, the local base station can send sensor data and an alarm to a central monitoring station if data indicating an anomaly in vital signs develops. This enables the medical staff at the central monitoring station to give the patient the best care possible. Information is transmitted between the patient and the monitoring facility over the Internet. This type of device just marginally restricts the patient's daily activities while allowing for continued observation of the patient.

C. Integrated System:

The two systems can be integrated to maximize the potential of these technologies. Once delivered to the central monitoring station, the sensor data can be included into the patient's EPR. By providing a more thorough explanation of the patient's medical condition, this information can help improve the delivery of medical health.

3. Security and Privacy (S & P) Issues:

To increase the overall quality of medical health delivery, the advantages of the aforementioned technologies must be assessed against the user's (S & P) concerns. The electronic transfer of medical records and data from patient wearing sensors will take place across wireless networks and the Internet. The threat to people's (S & P) is increased as a result, which is what this section focuses on.

A. Storage and Access to Data:

Concerns over the privacy and confidentiality of a patient's medical records have existed for a while [8]. Compared to paper-based medical records, personal medical health information is more susceptible to harmful attacks when connected to the Internet. Currently, getting a patient's medical record requires them to physically visit a medical facility. The amount of persons who can see the records and the way they are transmitted are physically constrained by the fact that they are in paper format.

However, once this information is made public electronically, it can be accessed by both legitimate users and malicious attackers. Additionally, because to the scattered nature of sensor networks used for patient monitoring outside of hospitals, it is more challenging to guarantee data confidentiality and integrity as compared to the traditional healthcare system. The wireless transmission of sensor data makes eavesdropping and skimming both possible. When wearable sensor networks and EPRs are used, access, storage, and integrity issues arise. The following inquiries must be addressed in order to solve the difficulties presented by electronic data and remote information transmission:

- ✓ To whom the data belongs to?
- ✓ Who is the in charge of upholding regulations governing the handling of medical health data and has the authority to remove, modify, and add data to it?
- ✓ Are the records of the patients personally owned by them?
- ✓ Do their doctors possess the data?
- ✓ Exist any insurance firms that own the data?
- ✓ Are they all co-owners?

A particularly complicated and unresolved problem is who actually owns the data. Legislative inquiries and continuing, well-publicized lawsuits have been centered on it. Additionally, some health maintenance organizations(HMOs) have started declining to pay for a patient's expenses when the patient has used experimental clinical treatment techniques [9].

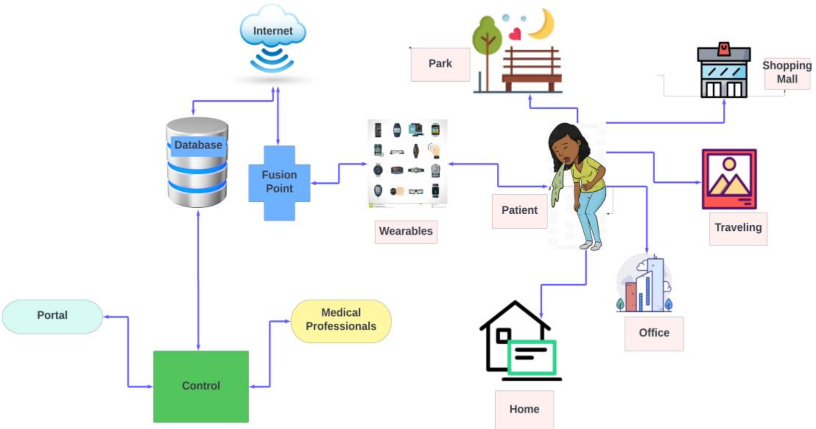

Figure-1: Remotely Monitoring of Patients

This raises the question of whether the insurance company can decline to pay for costs related to the gathering and storage of the patient's data if it does not control the data itself. This issue also has an impact on third party rights.

- ✓ Do recipients of data from the data owner enjoy the same rights as those recipients, or are those recipients' rights more restricted?
- ✓ What level of security and privacy protection must be maintained while sending data to a third party?
- **What kind of data, and how much of them, ought to be stored?**

Doctors' notes, MRI findings, and the outcomes of laboratory testing are all preserved in a patient's paper-based record. Will a part of the information in EPRs be enough to meet medical demands, or should all of it be kept electronically? For instance, data may be combined, and the information that results may be adequate for EPR users.

This study also addresses the usage of sensor networks for remote patient monitoring. For instance, only the aggregated data required for diagnosis and emergency response should be sent back to the monitoring center, while the remaining raw data should stay on-site at the patient's base station. The central site must only keep the amount of sensor data necessary to carry out the patient medical care-related tasks. The patient's care won't be significantly impacted by any further information, but it could jeopardize their privacy. In both instances, it is important to reduce the amount of data that is collected and retained while maintaining the appropriate level of medical care.

- **Where the medical health information should be kept?**

The difference between centralized and decentralized storage is at issue here.

Should data be kept in a central database or local databases that can be connected to one another in the case of EPRs?

Should the primary monitoring facility also store the raw sensor data for remote patient monitoring, or should it only be retained locally? What type of data storage will meet the (S & P) needs the best?

- **Which individuals have access to a patient's medical record file?**

The two groups of EPR users are: a) those with read/write privileges, such as doctors and nurses, who can access and modify a patient's (EPR); and b) all other users. b) Users with read-only access, such the insurance provider, who may only be allowed to view the patient's EPR without having the ability to make changes to it.

There might be further constraints on the parts of the data that a user's privileges apply, depending on the user accessing the EPR.For instance, an insurance company could be able to restrict access to EPR features that make it easier to pay for medical expenses. Another situation concerns a senior patient who wants to provide specific family members access to certain parts of their medical data.

- **Should this information be shared with anybody else without the patient's permission?**

There are circumstances where it is necessary to reveal a patient's medical health information to individuals who were not previously authorized users. For instance, when a patient is being monitored remotely, it may be necessary to disclose medical health information without the patient's permission in the event of an emergency so that the patient can receive the medical care they require.

B. Data Mining:

Data mining is the process of examining data to discover patterns and/or correlations. Human medical data are among the most gratifying and difficult biological data categories to mine and assess. It may be difficult or impossible to glean insights from studies on animals, but data mining on human beings can do, so it may be challenging to infer from studies on animals how pain, discomfort, and other emotions are perceived by animals [9].However, specific (S & P) rules that restrict the information that may be gathered, shared, and assessed apply to the mining of human data. Large amounts of medical data cannot be mined because they are no longer stored electronically. Nevertheless, each year tens of thousands of terabytes of digitized human data are generated in North America and Europe. Despite the fact that data mining on this information creates (S & P) problems, what can be done is limited by the diversity of the databases and the dispersion of the data among medical care facilities without any standard format or organizational principles. More healthcare institutions will have databases that hold patient data in a common digital format as EPRs become more common.The pool of human medical data can then be conveniently exchanged with the aid of the communication network. Due to the increase in data availability, it is necessary to assess the role and governance of data mining.

Medical data analysis may make it possible to categorize and characterize people based on things like age, gender, or condition. This may have ramifications for exclusion and discrimination. Data must be anonymized prior to any data mining because it can be moved and accumulated more and more like a "commodity" through the Internet. The definition of anonymity and the guidelines for data disclosure to users, such as managed care evaluators and insurance companies, must be made clear through data mining. It is possible to anonymize data in a variety of ways. For instance, removing personal identifiers like a person's name, age, or social security number may make it more challenging to link certain pieces of information to a particular individual. Even now, the data cannot potentially be sufficiently anonymous to prevent discriminatory effects. Despite not being directly linked to a single person, the data may be related to a larger sub-population, such as people who live in a specific location or persons of a specific gender or race. Determining how much anonymity is required for a specific data mining activity is therefore critical. As a result, the issue of whose access to the data and how anonymously it should be handled is brought up.A type of identification tag may be present in the data from a PC used for patient monitoring to allow the hospital know which patient's data it belongs to.The insurance company does not need to know the patient's identify, but the doctor may later need to mine the data. How much education do different providers have? How far should different providers be allowed to extend their data mining capabilities, There is no clear definition of what constitutes ethical behavior for the wide variety of disclosures made to secondary users, like insurance companies and managed care evaluators. To maximize the advantages of having more medical data available while avoiding unfavorable effects, these data mining-related challenges must be assessed and constraints placed in place.

C. Contradictory Regulatory Framework:

The American Health Insurance Portability and Accountability Act (HIPAA), in addition to federal legislation and other state regulations, is only one example of the numerous laws and regulations that currently control the medical and healthcare sectors. These guidelines give a structure for policy, but they will need to be adjusted if EPRs and sensors change the way that medical care is delivered.

Doctors, hospitals, and other healthcare providers must abide by the HIPAA laws. All patient accounts, medical bills, and data must adhere to a set of standard documentation, handling, and privacy criteria as outlined by HIPAA. Every patient must have access to their own medical records under HIPAA requirements, be made aware of any inaccuracies or omissions, and have the authority to change that information as necessary. Informing patients of privacy policies is one of the other HIPAA obligations [10]. The State of Health Privacy report from The Health Privacy Project does a great job of summarizing the specific regulations that each state has in place for the management of medical care [11]. HIPAA mandates that all patients have access to their own medical records, are informed of any errors or omissions, and have the power to modify that information as needed. The distribution of information to patients regarding specific medical disorders, such as mental health issues and sexually transmitted diseases, as well as the publication of this information, are, however, governed by unique laws in Alabama. The legislation in Alabama forbids HMOs from sharing patient information. Contrarily, California law guarantees patients' access to the medical records that government agencies, HMOs, insurers, and healthcare providers release to them. The distribution and use of medical health information by these businesses is likewise subject to a number of restrictions under California law.

As sensitive personal health information becomes more accessible electronically, it is important to have consistent procedures in place to safeguard it. Due to the different state laws, there are concerns around data ownership, access rights, and disclosure because data may be electronically transferred over state lines. A nationwide standard for health privacy is based on the HIPAA Privacy Protection Regulations from 2003 [10].

However, they are a very basic set of rules. They act as a "baseline" with the most basic consumer protections, with stronger or tougher state laws still in effect. Later, states may choose to enact stricter measures For instance, a patient's consent is not required in accordance with the HIPAA Privacy Protection regulations before moving their medical records from one doctor's office to another for treatment. The patient may have unmet (S & P) expectations if the state regulations governing the disclosure and use of this information are stricter in the patient's state than in the state from where the data is transferred Even while paper-based medical records are still a viable option, switching to electronic records makes it easier and more practical to move more data between states.

4. Solutions:

In this section, we go over these (S & P) issues current remedies as well as unanswered research topics.

A. Current Solutions:

Issues with data access, storage, and analysis are not unique to the medical sector. Technical options are available for the medical field of health care to enhance (S & P) in a multi-user setting. These challenges have been studied across a variety of sectors, including internet retail and financial services:

- **Role-based access control:**

One of the most challenging aspects of managing huge networks is its complexity [12]. Role-based access control, commonly referred to as role-based security, is the method of sophisticated access control that is most widely used.For big networked systems, a reduction in the cost and complexity of security administration is advantageous. Is an illustration of a role-based access control system for the medical healthcare industry?[13]

- **Encryption:**

Data confidentiality can be protected and eavesdropping and data skimming can be thwarted by encryption. Both hardware and software can be used for encryption. Utilizing both types of encryption will give you the highest level of security. Software can use a variety of symmetric and asymmetric key techniques to offer encryption [14]. To enable encryption and authentication in sensornet works is one of Tiny Sec's [15] main objectives. Tiny Sec is being used in several medical sensor systems, including the Kansas State University/University of Alabama in Huntsville WBAN.

- **Mechanisms for Authentication:**

To ensure that the data genuinely comes from the person or organization it is claiming to be from, authentication techniques can be utilized [14]. Passwords, digital signatures and challenge-response authentication protocols are only a few of the numerous authentication strategies that have been created. There are methods for conserving energy, such as Tiny Sec's hash function, which supports authentication and was created for sensor networks.

B. Future Work:

There are ways to aid with the (S & P) of medical data with the help of new technology, but there are still certain things that could be done better.

- **Identify the clear criteria for role-based access:**

The exact rules for role-based access must be specified in order to implement these systems. These may be static rules or dynamic rules, depending on what is required.

- **Making policies:**

A new policy that can address issues impacting several states must be developed. Despite the fact that the HIPAA Privacy Rules offer some framework, more work needs to be put into developing specific regulations that customers can rely on. It will be possible to communicate enormous volumes of data fast since EPRs are developing and distant sensor networks will be able to collect and store an increasing amount of medical data. This necessitates the creation of a complete set of rules that guarantee the (S & P) of users regardless of the location where the data is kept. In the current climate, many people lack knowledge of and are uncertain about their rights to medical data privacy. If clear regulations are not established, consumer confusion will worsen as more medical data is computerized and easily shared.

- **Guidelines for patients privacy:**

Does the patient have complete control, or just some of it, over how much information is delivered to the central monitoring station?

There must be rules established that specify what sensor data gathering implies and who will be in charge of it.

- **Guidelines for data mining and technology safeguards:**

These specify not just who has the authority to analyze what kinds of data, but also how the data should be anonymized. If automation is a possibility, the proper technical means for guaranteeing these principles must be implemented.

5. Conclusion:

People can now access medical health records online and store electronically in EPRs. The notion of remote patient monitoring is also becoming a reality with sensor network technologies. In the field of Medical health this is very hot topic for researchers to research as (S & P) is very important factor for the developer and adopter of Internet of Medical Things. The (S & P)is the basic and important requirement of all the Medical health care industries because it directly deals with the life of patients and there is nothing important rather than human life in this world. This study explored the (S & P) issues that come up while integrating this new technology into the current medical healthcare system. We looked at some of the now workable solutions and the remaining research issues that need to be resolved before the new technology can be widely deployed with the least amount of (S & P) risks.

References:

[1] Jiang, P., Qiu, B. and Zhu, L. (2022) “FastPRS: Augmenting fast and hidden query in EPR systems via online/offline puncturable search,” *IEEE Internet of Things Journal*, 9(2), pp. 1531–1541. Available at: https://doi.org/10.1109/jiot.2021.3089587.

[2] Ren, L. and Peng, Y. (2019) “Research of Fall Detection and Fall Prevention Technologies: A systematic review,” *IEEE Access*, 7, pp. 77702–77722. Available at: https://doi.org/10.1109/access.2019.2922708.

[3] Tandon, A. *et al.* (2020) “Blockchain in Healthcare: A systematic literature review, synthesizing framework and future research agenda,” *Computers in Industry*, 122, p. 103290. Available at: https://doi.org/10.1016/j.compind.2020.103290.

[4] Shah, S.M. and Khan, R.A. (2020) “Secondary use of electronic health record: Opportunities and challenges,” *IEEE Access*, 8, pp. 136947–136965. Available at: https://doi.org/10.1109/access.2020.3011099.

[5] Cilliers, L. (2019) “Wearable devices in Healthcare: Privacy and Information Security issues,” *Health Information Management Journal*, 49(2-3), pp. 150–156. Available at: https://doi.org/10.1177/1833358319851684.

[6] Liu, Q., Mkongwa, K.G. and Zhang, C. (2021) “Performance issues in wireless body area networks for the Healthcare Application: A Survey and Future Prospects,” *SN Applied Sciences*, 3(2). Available at: https://doi.org/10.1007/s42452-020-04058-2.

[7] Sudhakar and Kumar, S. (2020) “An emerging threat fileless malware: A survey and research challenges,” *Cybersecurity*, 3(1). Available at: https://doi.org/10.1186/s42400-019-0043-x.

[8] Koren, A. and Prasad, R. (2022) “IOT health data in Electronic Health Records (EHR): Security and privacy issues in ERA OF 6G,” *Journal of ICT Standardization* [Preprint]. Available at: https://doi.org/10.13052/jicts2245-800x.1014.

[9] “Security protocols with conventional cryptography” (no date) *A Classical Introduction to Cryptography*, pp. 135–153. Available at: https://doi.org/10.1007/0-387-25880-9_5.

[10] Naranjo-Hernández, D. *et al.* (2018) “Past results, present trends, and future challenges in intra body communication,” *Wireless Communications and Mobile Computing*, 2018, pp. 1–39. Available at: https://doi.org/10.1155/2018/9026847.

[11] *This domain name has been registered with Gandi.net* (no date) *healthprivacy.org*. Available at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm (Accessed: November 8, 2022).

[12] Cilliers, L. (2019) “Wearable devices in Healthcare: Privacy and Information Security issues,” *Health Information Management Journal*, 49(2-3), pp. 150–156. Available at: https://doi.org/10.1177/1833358319851684.

[13] Chen, W. *et al.* (2021) “If you built a sandbox: How children, network diversity, and community interventions are related to Google Fiber Signup in disadvantaged urban communities,” *Telematics and Informatics*, 60, p. 101580. Available at: https://doi.org/10.1016/j.tele.2021.101580.

[14] Coyne, E.J., Weil, T.R. and Kuhn, R. (2011) “Role engineering: Methods and standards,” *IT Professional*, 13(6), pp. 54–57. Available at: https://doi.org/10.1109/mitp.2011.105.

[15] Dinh-Le, C. *et al.* (2019) “Wearable Health Technology and Electronic Health Record Integration: Scoping Review and future directions,” *JMIR mHealth and uHealth*, 7(9). Available at: https://doi.org/10.2196/12861.