A Survey of Cybersecurity Vulnerabilities in Healthcare Systems

Adwan Alownie Alanazi
a.alanazi@uoh.edu.sa
University of Hail, KSA

Abstract
In the process of remarkable progress in the medical and technical field and activating the role of technology in health care services and applications, and since the safety of medical data and its protection from security violations plays a major role in assessing the security of health facilities and the safety of medical servers Thus, it is necessary to know the cyber vulnerabilities in health information systems and other related services to prevent and address them in addition to obtaining the best solutions and practices to reach a high level of cybersecurity against attackers, especially due to the digital transformation of health care systems and the rest of the dealings. This research is about what cyber-attacks are and the purpose of them, in addition to the methods of penetration. Then challenges, solutions and some of the security issues will be discussed in general, and a special highlight will be given to obtaining a safe infrastructure to enjoy safe systems in return.

Keywords
healthcare; cyber security; attack; malware; patient; threat; Access data; attacker; vulnerability; malicious program; approach; authentication; challenges; intruder; encryption

I. INTRODUCTION

Recent developments in the field of information technology have given rise to many networks and applications. In this regard, security is the primary concern to ensure complete communication between devices passing through network systems.

The technology is widely used in critical national infrastructures. With the integration of communication, computing and control technologies, cyber-attacks have become one of the main threats to systems in general. Take the health care system for example, the security incidents associated with health care systems in 2020 have spread fantastically, especially in light of the COVID-19 pandemic]. Recent incidents have shown that a cyber-attack can cause serious material damage to infrastructure in general and to health systems in particular. Consequently, it is important to focus on developing solutions to address these attacks, and to monitor and monitor systems to detect and respond to or prevent any infringement in order to ensure the safety and privacy of the confidentiality of patient data and not to seize or tamper with it.

After explaining the attacks and focusing on the capabilities of the attackers and knowing the purpose of carrying out the attack, the challenges of health care in terms of cybersecurity and the protection of basic data based on service provision and quality, whether at the level of systems or medical equipment, must be addressed.

The deployment of modern technologies in the health care sector without taking into account the aspect of privacy, confidentiality and data security makes the patient's privacy vulnerable. In fact, disclosure of information and the state of the disease sometimes may cause the patient to have problems in his social or professional life, or at other times, difficulty obtaining medical insurance.

Therefore, the urgent and explicit need to protect the confidentiality and integrity of health care systems' information and its availability in a timely manner are the main challenges.

In this paper we will discuss health care system attacks. The remainder of this paper is organized as follows: Section 2 provides an explanation of the impact of various attacks on the healthcare system while Section 3 describes an overview of the organizational and technical challenges facing e-health care systems. Section 4 provides an overview of some of the requirements to ensure the safety and privacy of healthcare systems and their related applications at several levels. In the fifth section, some technical practices are proposed as a kind of technical solutions to address or prevent cyber-attacks on health care systems, while in the sixth section the researcher gives an overview of some security issues in the health field and explains their impact and consequences on various fields.

II. CYBER ATTACKS IN HEALTHCARE

Due to the remarkable development in healthcare services and their dependence on technology, they are vulnerable to cyber-attacks that are intentionally or unintentionally executed for various purposes, either for the purpose of profit, controlling or tampering with the system.

Which affects the performance of health care systems in general, the performance of the network, and the databases where the patient's health records are kept, it is possible that this data may be attacked and seized by malicious hackers and thus breach the trust between the healthcare provider's

Manuscript received June 5, 2023
Manuscript revised June 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.6.19

system and the patients. The execution of a cyber-attack depends on the type of vulnerability that will be used to execute the attack and at what stage the vulnerability exists. And because the applications and devices used in the current health care systems are facing difficulties in achieving security and privacy requirements, which allows attackers to exploit the different components of health systems to carry out their harmful activities.

It is very important to know the capabilities of the attacker to successfully carry out various attacks targeting health care systems, as the specialists consider that knowledge of the opponent's capabilities is an important factor to counter the attack and thus restore order.

(1) The attacker is able to physically or remotely access the healthcare systems environment.

(2) The attacker is familiar with the communication standards and protocols used in health care devices and systems in order to establish communications with the programmed device.

(3) An attacker can access communication channels by using third-party devices.

(4) The attacker is able to impersonate a patient to collect sensitive information from the health care system.

Depending on the targets of the attackers, their capabilities, and their relationship to the health system, attackers can be classified in health care systems into two types:

(1) Passive Attacker: This attacker threatens the confidentiality of communication channels bypassing the communication channel authentication by eavesdropping on side and unintended communication channels without interrupting the communication. By reading the messages, he can identify and know the device model, the serial number, and reveal the patient's private information. In underground markets the value of patient personal health information is extremely valuable. Therefore, private information can be obtained if it is not protected and an authentication mechanism is imposed for that patient data.

(2) Active Attacker: This attacker is able to read, modify and pump all data by interrupting the communication channel. In addition to capturing exchanged messages. An active attacker can impersonate a programmed by a medical device, which is a third-party device often used in an IMD. Thus, he can reprogram the medical device and request sensitive information, or the medical device battery consumption. The opponent may also spy on the patient's private data (patient location, diagnosis) and use it to blackmail the patient and cause physical or psychological harm by infringing on his privacy.

We will discuss the current types of security and privacy attacks on health care systems and the various components of them, and then conclude how attackers can breach the security of health care systems and endanger sensitive data. With clarification of the methods of each attack and its effects on the victim.

To carry out any malicious activity, the attacker can target a computer or medical device, with the aim of intercepting communications, modifying data, lack of data availability, violating privacy, and so on. Based on the effects of the attack on health devices and its effect on patients, we will mention some of the types of attacks:

- Phishing Attack: An illegal email link that the attacker sends to the patient with the purpose of updating his health information. Where those emails make unrealistic threats or demands to click, it continues to cause havoc healthcare systems and networks by using some common phrases such as 'urgent action required' or 'to view your next appointment', also they may ask you to send money for expenses.

- Brute-force Attack: includes a trial-and-error method of guessing the password of system users. If the attacker has complete information about the opponent, then this attack is very simple.

- Keylogger Attack: By allowing a malicious attacker to capture keystrokes in the system. The attacker obtains the credentials for illegal access to the patient's health information based on the data that was captured by the key recorder, knowing that it is in the form of hardware or software.

- Man In The Middle Attack: One of the common attacks that occur at the network level where the attacker impersonates one of the communication parties in the network and gain access to the patient's database or the server.

- **Eavesdropping Attack:** is an interception that occurs by accessing the health report of illegally illegally connected patients in the network.

- Pharming Attack: This attack is related to a phishing attack where the malicious codes are installed in the victim's system and by hacking the DNS server the malicious website is executed.

- Denial of Service Attack DoS: One of the most common network attacks, it occurs by flooding the health care system with repeated, unwanted requests as the attacker picks up the network, allowing the attacker to capture the entire network. Therefore, legitimate users are not allowed to access their accounts or data in the health care system due to this attack that destroys access and overthrows the system.

- SYN Attacks: An attack that occurs by exploiting the TCP three-way handshake when sending data, as more than one handshake request is sent, thus bypassing the limited buffer space and thus the target system ignores legitimate sent requests.

- Data-tampering Attack: The attacker changes records through simulation as a legitimate user. This modification may damage the patient's health record**.**

- Jamming Attack: A type of attack that allows an attacker to run WiMAX frames within short periods of time. Attackers can distinguish the network and thus confuse the entire typical operation of a network.

- Scrambling Attack: By means of communications eavesdropping devices, the attacker tampers with the network and monitors phone calls and all movements within the network.

- Password Attack: occurs through a breach of the patient's health record and thus access and control of the health system is possible.

- Buffer Overflow Attack: An attack in which a program overwrites the cache adjacent to the store that should never be modified. Often times a program crashes when a buffer overflow occurs in a program or stops working.

- Weak Authentication Attack: Unauthorized access to existing data by exploring vulnerabilities in the system and a backdoor for the attacker to gain access.

- SQL Injection Attack: one of the most popular attacks where the attacker injects malicious SQL statements into the database in order to explore the security holes in the system and thus exploit them to access the patient's health record and modify or hijack it.

- Session Hijacking Attack: The attacker takes the session between the client and the server. This is done by replacing the attacker's computer Internet Protocol (IP) address with the client's computer address, and the attacker continues using the server in the connection session without noticing it. This attack is effective because the server uses the client's IP address to verify its identity.

- Trojan Attack: The attack uses a malware hidden inside another, apparently legitimate program. So that when the user runs the program that is supposed to be a healthy program, the malware can be used in a Trojan horse attack to open a back door in the system that allows hackers to penetrate the computer through it.

TABLE I. Cyber -Attack on Healthcare System

Device	Attack	Parameter	Result
Therapeutic equipment	**Spoofing**	Dosage protocol *	Incorrect amount of dosage or concentration administered to the patient
		Purge rate	Altering the purge rate of the air inside the pump
		Pressure	Pump stops from administering medication
	Malware	Alarm	In case of failure, the alarm is setto off
		Monitor display informatio n	Modification of correct information regarding dosage or patient profile
	Malware or DoS	System reboot	Configuration is changed to default
		PET	The image files of the patients are accessed by unauthorized third
	Intrusion attack	imagefiles / X- ray image files	party that can held a lock upon these files asking for ransom in return or to extract them in order togain financial benefits or just to delete the entire database
	Malware	Alarm	Mute all alarms in case of failure or critical levels of radiation
	Malware /SQL injection	Image files	Associate PET image with the wrong patient's folder
	Malware or DoS	System reboot	Configuration is changed to default
	Malware	Change settings and diagnostic protocol procedure s	Incorrect diagnostic procedures in the memory of the machine (PET scanner)
		Voltag e(kVp)	Increase voltage determining an increase in keV photons of the X- ray machine
		Curren t(mA)	The current increasing determinesan increase in the quantity of photons (X-rays)
		Monito r display information	Modification of correct information regarding dosage or patient profile
Surgical machines	**Malware**	Informatio ndisplay	Confuses the surgeon while reading status data of the patient (heart rate, arterial pressure, temperature etc.)
	Malware Or DoS	Syste m reboot	Configuration is changed to default and can happen during the surgicalprocedure in a critical moment.
		Angle of arm rotation, lateral movemen t distance	Patient life is threatened due to incorrect response of the robot being control by the surgeon
	DoS	Networ kpacket	Network packets of the commandscan be dropped and delays can occur

III. ATTACKS APPROACHES

To understand how the impact of attacks is determined. Note that the following vulnerability models are to illustrate the different types of attacks and their impact on health care systems:

1- ***Attack Method (AM)*****:** This technique describes how the attacker exploits the health care system and carries out the attack. Based on that, passive attacks can be referred to as carrying out harmful activities in the health system without

interfering with the normal operation of the system, in contrast, active attacks impede the normal operation of the health system to carry out the malicious attack.

2- Attack Complexity (AC): This approach limits the amount of information about healthcare devices the attacker needs to carry out the attack, partial information (type of device, protocol used) or complete information (network architecture, type of encryption used).

(3) Privilege Requirement (PR): The attacker needs certain privileges to execute an attack, so that he uses privilege to access the system to explain the effect of the attack. For example, a packet-sniffing attack does not require any system access to carry out the attack, whereas an impersonation attack requires access to system tools.

(4) User Collaboration (UC): A human actor is sometimes required to successfully exploit the vulnerability. For example, user interaction is required to install the malware in a health care system.

I. CHALLENGES AND ISSUES OF HEALTHCARE SECURITY

Recently, electronic medical systems are widely used in many applications, so it is important that the security features of these systems are of great importance to those responsible. Working towards fair solutions in the critical infrastructure of these systems would have dire consequences.

Having efficient and effective security countermeasures in cyber systems is essential to overcome various attacks. Failure to properly perform updates in control systems against cyber-attacks. Some of the new research challenges in health systems are software with high assurance, security, privacy, and reliability.

Some of the challenges facing cyber-physical systems are related to the extent of adaptability, portability, and inconsistency with the system's tools, performance, reliability, flexibility, reliability, and ability to maintain these systems. In short, medical-physical systems open many doors for researchers and industries to overcome data security and privacy concerns.

A. Readiness assessment and resistance to change:

The first challenge facing the health sector is to conduct a reliable assessment of the readiness of the electronic health information system, to assess the communication infrastructure, and to evaluate the human resources, legal affairs, and command and control departments in relation to health activities, so that this assessment is a tool for gathering information for strategic planning for the future. Resistance to change is expected to come from denial of need, rejection, lack of awareness of success, or fear of failure to make the change.

B. Integration between public health and clinical care and confidentiality and privacy:

Many medical records systems are still paper and incomplete, and so far, not all hospitals have implemented electronic medical records systems and archive medical data. The biggest challenge is how to ensure effective electronic sharing and exchange of medical information and integration between health departments and clinical care activities.

C. Identification and profiling the end -user segmentation:

One of the future challenges of implementing a health information system is the heterogeneity of the end-user group. Therefore, the health system must be defined and designed to distinguish the end-user segment. This will require analyzing huge data sets, as well as using a mixture of demographic and health variables, as this is another challenge.

D. Monitoring and assessing the impact of IT and mobile media on physical medical systems:

The widespread accessibility of smartphones has led to a focus on audience participation through applications and platforms that can be accessed remotely using the network outside the health organization. There are thousands of health apps, and although these apps are useful, users do not reflect the positive nature and commitment to using them.

II. SECURITY AND PRIVACY REQUIREMENTS FOR HEALTHCARE SYSTEMS

Healthcare systems include additional security requirements that contribute to ensuring privacy and raising the level of systems security. Each level of healthcare systems has different tasks and requirements for security and privacy.

A. DATA LEVEL

1) Confidentiality: The collection and storage of patient health data must comply with legal privacy regulations, such as the General Data Protection Act and the Health Insurance and Liability Transfer Act (HIPAA). This means access to data for only authorized individuals to prevent data breach, and necessary measures must be taken. To ensure the confidentiality of individuals' health data. It must be stressed the importance of implementing these measures to limit the sale of stolen data in illegal markets, and the consequent suffering of patients and the violation of their privacy, not to mention financial damage. Therefore, caregivers must comply with the General Data Protection Regulation (GDPR) and obtain the consent of patients when exchanging any health information Protected with other health care centers.

2) Integrity: The main goal of meeting data integrity requirements is to ensure that the transmitted data arrives and that it is not penetrated during the transmission process. Since the ability to detect potential attacks or manipulate data in any form is critical. Therefore, necessary measures must be implemented for data integrity, in addition to ensuring the safety of the data transferred and stored in medical servers from modification or change by attacks.

3) Availability: Means the ability to access data when it is needed from authorized users. While the lack of access to data sometimes leads to life-threatening accidents, such as the inability to provide an alert for the occurrence of a heart attack in the hospital or the inability to know the medical history of an emergency patient. Therefore, to ensure data availability and emergency services the healthcare system must always be operational. Medical service providers must also be able to restore availability or access data in a timely manner.

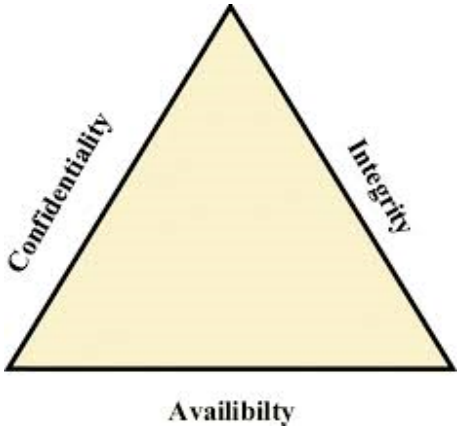

Fig.2. CIA triangle

B. SENSOR LEVEL

Security at sensor level faces most of the challenges in the healthcare system due to limited power limitations for medical equipment and sensors. Sensor level safety measures should be lightweight, cost effective and affordable.

1) Tamper-Proof-Hardware: Theft of surrounding sensors results in security information being exposed to a cyber-attack. The attacker might reprogram the stolen devices and re-deploy them to the system again, thus he could listen to the communications without noticing it. Therefore, physical theft of medical devices is a serious security threat and needs to be addressed in healthcare systems.

2) Localization: There are two types of sensor localization, the position of the sensor on the body and the location of the sensor in an indoor environment. Determining the position of the sensor on the body is important for applications such as activity recognition, for locating the sensor or for determining the location of the patient wearing the sensor.

3) Over-The-Air Programming: Remote update has become a common way to update systems from sensor nodes, which present security concerns such as malicious sensor node listening updates so appropriate security measures must be taken to prevent attackers from exploiting those updates.

C. PERSONAL SERVER LEVEL

Because patient data is stored and collected on a personal server before it is sent to medical servers in health care systems, and to ensure the protection of data and privacy while it is on personal servers, two types of authentication systems must be applied, device authentication and user authentication.

1) Device Authentication: The server performs authentication before receiving data sent from the medical devices. The authentication must be able to establish a secure and encrypted connection for the integrity of the data. Mostly, hardware authentication is mutual between main servers and personal devices, but the majority of mathematical operations are performed on personal servers, as they have computing capabilities and power that exceed medical devices.

2) User Authentication: Data stored should only be accessed by medical users and staff, therefore, medical servers must support emergency data access. The use of biometrics is a solution for personal server-level user authentication that applies in healthcare systems.

D. MEDICAL SERVER LEVEL

Two of the most important requirements for the security and privacy of patient data are: devices and authorized personnel. Only those who have access to the data, and the data must be encrypted when stored in the databases. Therefore, necessary security measures must be taken to maintain the safety and privacy of the medical server for health care systems.

1) Access Control: Effective access control systems must be deployed to ensure access to medical servers from authorized personnel. It is difficult to request patient consent every time an attempt is made to access data. Therefore, access control must be provided to medical servers, and data that can be shared without permissions must be specified in addition to the data that third parties are permitted to access. Attribute-based encryption, which is known as public key encryption, is a common solution to safeguarding data integrity from abuse, as permission to access encrypted data is only granted for a predetermined set of powers. A scalable policy update plan should also be posted to reduce algorithms in cryptography.

2) Key Management: The development of secure applications relies on key management protocols, and the goal is to implement and distribute cryptographic keys to sensor nodes. Trusted server protocols fulfill the basic agreement within a network and despite this, trusted server protocols are insufficient for critical applications because a complete network failure may destroy a trusted server in real time. To share secret keys before the network operates, master pre-distribution protocols are often implemented in symmetric key cryptography. Implementing these types of protocols is straightforward and does not require complex calculations.

3) Trust Management: A two-way relationship formed between two trusted nodes that share data. Distributed collaboration between network nodes is essential to the success of wireless healthcare applications. The level of node

trust can be determined through trust management systems because confidence assessment of node behavior is critical in healthcare applications.

4) Cryptography: In order to achieve security and privacy of data in the field of electronic healthcare, we need to apply symmetric and asymmetric encryption systems. Energy, memory space and execution time must also be considered.

5) Secure Routing: There are many security and privacy issues in all routing protocols. It is worth noting that designing secure protocols for wireless networks is a complex matter.

III. BEST PRACTICS TOWARDS DIGITAL HEALTHCARE SAFTY

In the past, intrusion detection systems (IDS) were used to identify patterns of intruders with the algorithms used to destroy systems in the medical field. With IDS difficult to install, it is also difficult to connect to MCPS driver systems. Symmetric coding was previously developed for implementation. This allows the computation and processing of texts and encrypted data, and thus the result is encrypted, the last result coinciding with the result of operations when decoding.

Among the tools and mechanisms used to detect attacks:

Hyper Network Model of Statistical Analysis System (SAS):

It has a simple structure with a protection scheme as well as other functions that are often used with other types of transmission substations. Each function contains the same number of logical nodes (LNs). It is a sub-function that exchanges data with separate logical entities in another location. In the SAS model, there is a function for a set of logical nodes that helps define the critical and sensitive data retrieved.

Virtual Private Network (VPN):

One of the modern solutions to counter attacks on health systems lies in the creation and implementation of a virtual private network (VPN), where that virtual network imparts a default character to the private network and then takes advantage of security solutions to provide secure communication over the network.

A VPN is an alternative to another private network. It is used to overcome IDS problems.

There are also new methodologies such as:

The EDADT algorithm, the HOPERAA variant, the IDS hybrid model, and the semi-supervised approach to counter attacks on health systems. Which mainly depends on the behaviors and details of databases to determine the natural patterns of any device and determine its behaviors. These algorithms and methodologies are used in testing medical sensor measurements to detect possible defects in physical properties due to infiltration.

The ideology of the interdisciplinary approach, in which robotics, artificial intelligence (AI) and medical knowledge are combined together, works to raise accuracy rates and thus increase the efficiency of these systems.

IV SECURITY ISSUES

Data is exchanged in health care networks like any other network, the health care network relies heavily on the integration of information and communication technology with all sectors of health care in order to ensure the quality of services provided to the auditors, so that this integration results in a complex system to identify strengths to strengthen them and potential weaknesses to work on To avoid them, and to develop strategic and effective methods to protect data and communication networks and prevent the following:

• Disruptive attacks that could potentially disable hospital systems, or vital medical equipment such as laboratory analyzers, or reset or restart the configuration settings in those devices.

• Theft or impersonation by stealing user records and thus using them as unlawful to achieve sabotage goals, and unauthorized access to controlled substances by impersonating a medical staff account.

• Loss of medical information for patients, which reduces the reliability of clients.

Communication technologies are an important factor in moving the medical field to a more advanced level, and through the physical equipment of the healthcare network, the safety of these technologies can be seriously affected.

It should be noted that the lack of an approved mechanism for access to medical equipment, such as emergency devices, laboratory equipment, is a serious danger and a vulnerability that attackers exploit for several purposes such as controlling it remotely to change dose rates.

The transmission of medical information over the network without its encryption makes it easier for attackers to intercept and manipulate it, thus affecting the level of service provided to the auditors in addition to losing confidence and most importantly, diagnosing based on this wrong data in the event that the attack is not detected by system administrators. Such as the patient's laboratory records or x-rays.

Therefore, it is important to take measures to ensure the protection of data in the health organization, such as:

- Set authentication and access control according to job role.
- Data encryption.
- Approval of the assessment of safety levels for medicinal products.

- Giving priority access to information systems and granting permission only to those authorized to access data and determining the validity of reading or modification according to the job role, for example, doctors can view the patient's record, diagnose, order laboratory analyzes and x-rays, and print medical reports from the authority of the paramedics.
- Implement key management between medical devices, computers and database servers to ensure confidentiality and reliability in communication.
- To maintain availability, a secure network communication architecture must be achieved by enabling the nodes connected to the network to become anti-attacks, securing individual routers from entering spurious packets, and enabling secure routing protocols from entering wrong path data, all of which results in securing the confidentiality and authenticity of communication between the two ends Connection.
- Install operating system security programs so that if malware is injected and administrative privileges are used to control the system, discovering that the code is legitimate or not is very difficult.
- It is important that countermeasures are able to deal with human error.

Accordingly, society will be more productive and lead economic growth if it enjoys health and the safety of the health network is guaranteed from exposure to electronic attacks, tampering and unauthorized access with the intention of accessing important information or even causing physical harm to inpatients and reviewers.

Reporting rules reduce information asymmetry by providing patients with information about security performance, so that information on security performance enables them to make the right choices based on their security preferences.

For example, it is likely that the technical resources of health-care centers that have more patient visits than centers with fewer visits, and thus have better security performance. Also, health facilities with integrated electronic health records should achieve better data protection. Therefore, attacks on the data could be linked to patient visits but without effect. Although the data breach did not affect the data, this led to a significant decrease in the number of outpatient visits to these health centers.

CONCLISION

Knowledge of attacks of various kinds and objectives can be used to predict risks and attacks in the future. In order to achieve this, we need to define the methods, methods and techniques that must be followed to deal with the large number of information and updates and the continuous development of technology at the same time. Thus, protecting assets from threats, in addition to being aware of the locations of weaknesses in health care systems, in order to be able to assess risks and find quick solutions. In the meantime, system administrators must work to routinely and continuously test the systems to discover any threat that might endanger the systems or the network and rectify the matter before the occurrence of the incident. Especially confirming that the data is an important target, so it must be emphasized that it is protected from violations and defining responsibilities and access powers, no objection. In internal user awareness testing to prevent unintended data leakage.

REFERENCES

[1] Dogaru, D. I., & Dumitrache, I. (2017). Cyber security in healthcare networks. *2017 E-Health and Bioengineering Conference, EHB 2017*, 414–417. https://doi.org/10.1109/EHB.2017.7995449

[2] Priya, R., Sivasankaran, S., Ravisasthiri, P., & Sivachandiran, S. (2018). A survey on security attacks in electronic healthcare systems. *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, *2018-January*, 691–694. https://doi.org/10.1109/ICCSP.2017.8286448

[3] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Selcuk Uluagac, A. (2020). A Survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ArXiv*, *1*(1), 1–40.

[4] Dogaru, D. I., & Dumitrache, I. (2016). Cyber-physical systems in healthcare networks. *2015 E-Health and Bioengineering Conference, EHB 2015*, 15–18. https://doi.org/10.1109/EHB.2015.7391368

[5] Nair, M. M., Tyagi, A. K., & Goyal, R. (2019). Medical Cyber Physical Systems and Its Issues. *Procedia Computer Science*, *165*, 647–655. https://doi.org/10.1016/j.procs.2020.01.059

[6] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access*, *7*, 183339–183355. https://doi.org/10.1109/ACCESS.2019.2960617

[7] Saleem, K., Zeb, K., Derhab, A., Abbas, H., Al-Muhtadi, J., Orgun, M. A., & Gawanmeh, A. (2016). Survey on cybersecurity issues in wireless mesh networks based eHealthcare. *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom 2016*. https://doi.org/10.1109/HealthCom.2016.7749423

[8] Chen, Q., Lambright, J., & Abdelwahed, S. (2016). Towards Autonomic Security Management of Healthcare Information Systems. Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016, 113–118. https://doi.org/10.1109/CHASE.2016.58

[9] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Based Medical Systems for Patient's Authentication: Towards a New Verification Secure Framework Using CIA Standard. *Journal of Medical Systems*, *43*(7). https://doi.org/10.1007/s10916-019-1264-y

[10] Bahkali, S., Almaiman, A., Almadani, W., Househ, M., & El Metwally, A. (2014). The state public health informatics in Saudi Arabia. *Studies in Health Technology and Informatics*, *202*, 257–260. https://doi.org/10.3233/978-1-61499-423-7-257

[11] Kwon, J., & Johnson, M. E. (2015). Protecting Patient Data - The Economic Perspective of Healthcare Security. *IEEE Security and Privacy*, *13*(5), 90–95. https://doi.org/10.1109/MSP.2015.113