Journal of Statistics Applications & Probability
An International Journal

http://dx.doi.org/10.18576/jsap/130129

Designing A Standard-Based Approach for Security of Healthcare Systems

S. Abuasal[1,], Kh. Alsarayra [2] and Z. Alyabroodie[2,3]*

[1] Software Engineering Department, Faculty of Information Technology, Zarqa University, Zarqa, 13115 Jordan
[2] Software Engineering Department, Faculty of Information Technology, Hashemite University, Zarqa 13115 Jordan

Received: 20 Mar. 2023, Revised: 29 Mar. 2023, Accepted: 28 Apr. 2023.
Published online: 1 Jan. 2024.

Abstract: Healthcare systems in recent years have had the highest cost of breaches. Data security is one of the most obstacles encountered in the healthcare system, which could cancel the integrity, availability, and confidentiality of medical data. These breaches are expected to increase in the future. Therefore, it has become necessary to develop systems that provide full protection for patients. Healthcare systems security can be improved greatly by involving security requirements in the early phases of system implementation. Usually, the security requirements are only handled from a technical viewpoint during the implementation phases. When building security in the implementation phase, this leads to weakness in system security and an increase in violations. So, this research paper is aimed to improve the security of healthcare systems, by focusing on security requirements in the early phase, and making the healthcare systems less vulnerable to hacking or any external threat by restricting access to healthcare systems. This research paper proposes designing a standard-based approach to the security of the healthcare system, which analyzes and combines system and software security requirements required to gain a secure healthcare system architecture. Both types of security requirements are designed in the healthcare architecture based on the COSMIC ISO/IEC 19761 standards. A case study is introduced for the proposed standard-based approach experimented by using the system and software security requirements specifications to protect the pharmacy system in the healthcare system from ransomware.

Keywords: Security requirements, Healthcare system architectural, COSMIC ISO/IEC 19761 standards, international standards.

1 Introduction

In recent years, the healthcare system has become an essential part of human life. Which caused a true revolution in the way the world works. The healthcare sector is affected positively by the revolution through enabling the medical institutions to observe patients and provide recommendations remotely [1]. Certainly, the priority in the healthcare system is the protection of patient data, which is regarded as extremely sensitive and personal information. All modifications or violations are not permitted which leads to a significant health threat for patients and big accountability for clinicians [2]. Also, it could result to real problems such as data breach and theft, scams, misconduct, and exposing patients to real risk, at

the end it may lead to death. Unfortunately, these changes occur to their data and medical history may remain undetected for years [3][4]. The security of data is one of the most obstacles encountered in the healthcare system, which could cancel the integrity, availability, and confidentiality of medical data [5]. Due to the increase of threats on the Personal Health Information (PHI), it has become necessary to develop systems that provide full protection for patients. Studies and research have indicated that PHI are highly vulnerable to malicious user attacks [6][7]. Security on critical systems is very serious, especially Electronic-healthcare (E-healthcare) systems which require more attention in this regard.

Security Requirements Engineering (SRE) is one of the most significant aspects of the achievement of secure software systems. Usually, the SRE faces problems like define the requirements specification without analysis [8], and the security requirements are just dealt from a technical viewpoint during the implementation phase [9]. However, security should be dealt with in all system development phases, precisely during the early phases, as well as the security goal can be achieved early in the analysis phase by analyzing the system architecture that provides the necessary functional requirements. Security requirements are usually considered a constraint on the system functions. Moreover, security requirements are regarded as Non-Functional Requirements (NFR) or quality requirements [10][11]. Increasing threats and attacks on software caused massive losses to many companies. Consequently, this led to failure in resisting cyber threats.

According to IBM Security's annual report [12] in 2021, data breaches showed that the year 2021 was the highest in the cost of breaches. Hence, the cost of data breaches grew from 2020 to 2021 from USD 3.86 million to USD 4.24 million, making it the costliest period in the previous 17 years. The average total cost of a data breach has increased by 10%. as shown in Figure 1. Which indicates that the security problem is inflating, and healthcare organizations must understand this

*Corresponding author e-mail: Sabuasal@zu.edu.jo

as soon as possible.

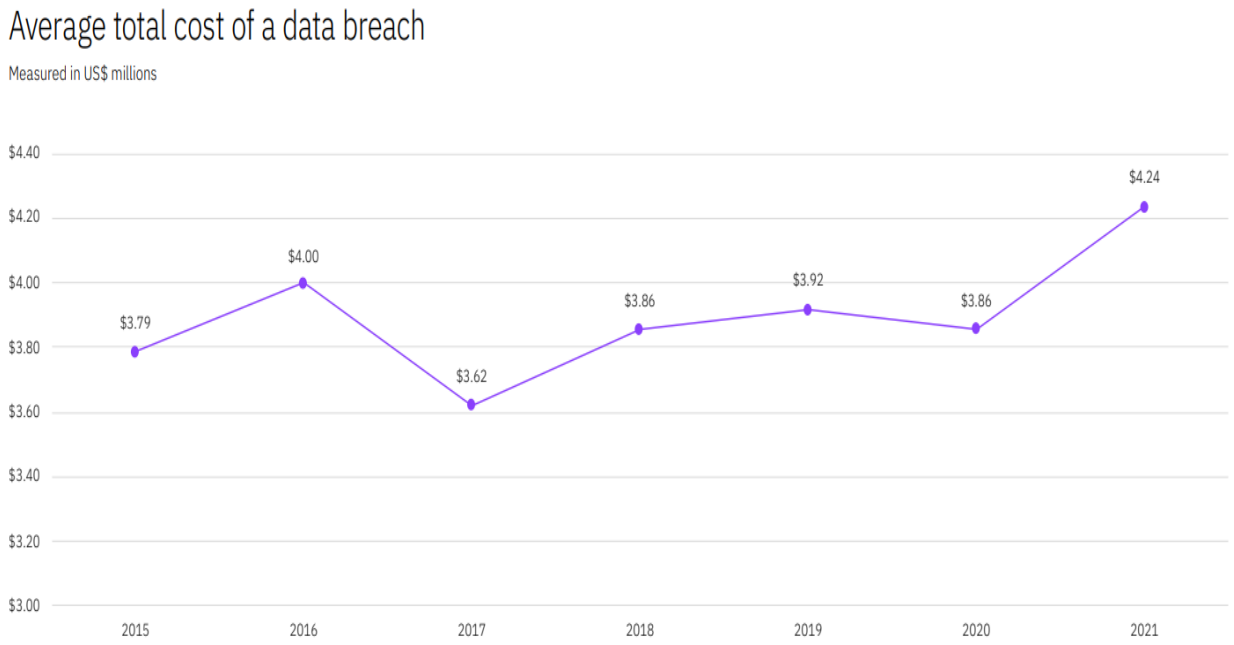

Fig. 1: Average Total Cost of Data Breaches - ref [12]

IBM's report shows that healthcare has the highest average breach rate in the last eleven sequential years. Costs associated with healthcare data breaches rose by 29.5 percent, from an average total cost of 7.13 million in 2020 to 9.23 million in 2021. The above-mentioned facts and figures in IBM's report indicate that the data of individuals and organizations are at risk.

More alarmingly, the healthcare industry, in special, is being targeted by attackers, because (PHI) is more valuable on the black market than credit card credentials or Personally Identifiable Information (PII) because its rich saturation of financial and identity information [13]. Therefore, there is a powerful incentive for attackers to target medical databases. The PHI can sale or use it for their gain. Some attackers get unauthorized access to prescription drugs using PHI for their own use or for selling. This has become a significant interest for the breaches of healthcare data. Though the data breaches are of various types, their impact is almost always the same.

The aspects of security failure have many reasons: high cost to secure the information, inability to integrate security in Software Development Life cycle (SDLC) in the correct form, especially in the requirements phase. Usually, an organization doesn't see itself vulnerable to a data breach [14].

Although PHI needs to be protected, security issues are unfortunately, neglected in most healthcare systems [15]. Also, the software engineers often fail to give appropriate attention to security concerns. The most major issue is that in almost all software projects security is dealt with when the system has already been developed and placed into operation. Therefore, this research paper contributions are to the increases the security of healthcare systems, by focusing on security requirements in the early phase, to the SDLC. The goal of this research paper is to make the healthcare systems less vulnerable to hacking or any external threat by restricting access to healthcare systems. Also, to give stakeholders a set of standards-based security requirements for designing secure healthcare applications. Whereas the objective of this research is to design a standard-based approach at a security requirements level for a healthcare security system to protect the system's information. This helps stakeholders make decisions during the requirements phase at an early stage of the identification, specification, and analyze for security requirements.

The remainder of the essay is organized as follows. The related works are presented in Section 2. Section 3 Identification of the system and software security requirements views, concepts, and terms. Also, it presents the E-healthcare architecture components and integrates them into COSMIC ISO/IEC 19761 standards. Section 4 presents a standard-based approach for specifying system and software security requirements for the E-healthcare architecture needed to make the healthcare system secure. Section 5 discusses a case study for the proposed standard-based approach by using the system and software security requirements specifications to protect the pharmacy system from ransomware. Finally, in Section 6 show conclusions and further work.

2 Related Work

This section includes a review of the academic literature on healthcare system security as well as related works on security requirements in the literature and international standards.

A. Security requirements in the literature and international standards

International standards describe security requirements as NFR. Whereas there are several concepts provided in the European Cooperation on Space Standardization (ECSS), the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE) that describe security. International standardizations are considered as a baseline for a description of security requirements.

In European Cooperation on Space Standardization (ECSS)[16] [17] considers security requirements as an NFR for systems and it is defined as the requirements baselines. While (IEEE) [18] are defined as an NFR. The IEEE security viewpoint has aspects that protect the software from anonymous access or change, or exposure to the system that could guide the destruction of that system. On the other side, the International Organization for Standardization (ISO) regards security requirements as a component of software functionality to assess the quality of the software product. Security is defined by the (ISO 9126 2004) [19] as the capacity of the software product to save information and data such that unauthorized persons or systems cannot read them or change them, and authorized persons or systems are not constrained to have access to them.

Unfortunately, often security requirements are not given sufficient concentration by organizations through software development. Usually, security is addressed after the software implementation phase, and it is ignored in the first phases of SDLC. Since security is generally defined as NFR, the organizations commonly release security fixes after the development has been completed, or when the security problems are encountered which often increases the risk of occurring security flaws [20]. So, many researchers have emphasized that attention to software security should be expended in the early phases of software development [21].

In the literature on security requirements, there are several published works. Some of these studies provide a framework for identifying and measuring security requirements, while others present methods for integrating security in SDLC, as well as identifying security vulnerabilities.

Based on international standards (the COSMIC ISO/IEC 19761) of the early specification and measurement of the non-functional and functional software security requirements, Abran and Al-Sarayreh [22] established a reference measurement framework for security needs. In addition, Al-Sarayreh et al. [23] established a framework based on international standards from the ECSS, IEEE, and ISO to identify, specify, and quantify software security requirements.

Meridji et al. [10] presented an approach for system security NFR by focusing on system security requirements to define a requirements framework of system security that is relying on international standards ideas compatible with ISO 19761 as a basis for the definition and measurements of FR. A framework to extract and assess security requirements was put forth by Haley et al. [24]. The three components that make up this framework are: identifying the security requirements; developing the context for the system; and developing the structure for satisfying arguments for verifying whether the system can satisfy the security criteria. Nazir et al. [25] conducted a study in which they reviewed security issues in SDLC and provide a set of tips that must be followed at each stage of SDLC to avoid violations. While Fernandes et al. [26] have integrated security into (SDLC) to identify security vulnerabilities and produce a highly secure product by testing the Internet of Things (IoT) health monitor. As a result, they found that if vulnerabilities are identified and addressed at an early stage in SDLC, huge costs for post-implementation remediation will be saved if any of the known health monitor vulnerabilities are exploited.

Nazir et al. [27] have focused on the development of IoT cybersecurity from ontological analysis and proposing suitable security services that are conformed to the threats. In order to strengthen security at the outset of system development, Aljawarneh et al. [8] presented a framework for cloud security requirements engineering with five fundamental tiers. Because it can be challenging to define needs in general, and security requirements in particular, at an early stage of system development.

B. Security of healthcare systems

Adil Hussain et al. [28] analyzed healthcare data breaches. The study discovered that hacking incidents are the most dominant forms of attack, followed by unauthorized internal disclosures. While Jiang and Bai [29] analyzed 1138 protected health information breaches from 2009 to 2017. As a result, they found that these breaches had affected 164 million patients. In fact, more than half of the cases of the breaches were not from External causes. They, however, were attributable to internal mistakes or ignoring. Also, Hicham et al.[30] presented an analysis that was performed on data

breaches for over 9000 data breaches encountered in various organizations from 2005 to late 2018. 11,5 billion unique records were lost as a result of these breaches. Also, they discovered that the most targeted type of organizations are medical organizations. While Ambarkar and Shekokar [31] studied the causes of breaches in healthcare systems and concluded that confidentiality and authentication are the most common two security goals that the system failed to fulfill. While Mamdouh Alenezi [32] proposed a framework that combines ontology-based security management with the development phases to provide healthcare web application developers with a methodical secure development pathway. Pramanik et al. [33] studied potential threats to the security of healthcare systems. They concluded that the biggest challenges facing healthcare systems are data deletion and the possibility of revocation.

Adamu et al. [34] proposed a web framework that prevent the popular security vulnerabilities in the Electronic Medical Record (EMR). Moreover, Shrestha et al. [35] Proposed a secured E-health framework, in this framework, access control scheme with enhanced encryption method has been considered and patient-centric personal data. Followed by, the many aspects that directly impact information security in healthcare online applications were assessed by ALKA et al. [36]. The security vulnerabilities of health organizations were recently identified by Ismail et al. [37], who also looked at potential ways to solve the issues raised. While Omer Kasım emphasizes the importance of adhering to security rules when accessing, writing, and updating electronic medical information [51].

Security requirements have been described by various researchers, and no standard definition has been agreed upon. We can observe that most of the security definitions are interested in designing secure software from early software development. According to previous studies, healthcare applications still take the largest share of breaches, and this shows that there is a real security issue that needs to be addressed. Also, the combination of sensitive patient information and vulnerability makes healthcare systems the most attractive targets for hack groups. Healthcare organizations must realize that they are very appealing to cyber criminals today. Therefore, both system and software security requirements of healthcare systems must be dealt with from the outset due to the sensitive data they carry. In previous studies, several researchers have studied security requirements in general. To improve the security level for healthcare systems, we have studied in this research paper the system and software security requirements commensurate with the healthcare system architecture to constrain access in the system and protect sensitive information.

3 Background

The preventive functions are determined at the early phase of SDLC to prevent the attackers from harming the system security. These preventive functions are only achieved when considering security requirements. There are two connected sets of security requirements. that should be considered at the requirements phase: system security requirements and software security requirements [10] [22]. In system security requirements, the security requirements are applied to all system components such as hardware and software. While, in software security requirements, the security requirements are specified for software within the system. We studied these two requirements to ensure that user access to the system is restricted, and that the healthcare system is secure. When applying the security requirements to the system; this is undoubtedly reflected in the components of the system, such as software, which becomes secure.

To ensure a higher level of software protection, should also implement security requirements at the software level.

A. System Security Requirements

When defining a system security requirement, three types of security requirements are considered , (i.e.) the CIA triad [Confidentiality, Integrity, and Availability][23]. The system can be considered secure if it achieves the CIA triad, as it is considered the heart of system security [38]. For data to be completely secure, these security goals should be achieved. Therefore, requirement engineers should understand and study these goals carefully. The CIA triad model helps to guide the development of security policies for organizations. Such a model considers any organization's security infrastructure and guides all the organization's efforts towards guaranteeing system security. A standard-based approach in this research paper identifies the security requirements terminologies and functions according to the IEEE, ISO, ECSS standards, and academic literature. System security requirements is divided into three security-related concepts (confidentiality, availability, and integrity):

- The ***Confidentiality*** aspect of the CIA triad ensures that pre- venting information access by unauthorized individuals, entities, or processes this requirement guaranty that health care system can prevent highly sensitive and critical information from reaching the hands of attackers. To restrict access, access control roles should be established in the healthcare system [23][39]. The key system confidentiality concepts are shown in Table (1).

Table 1: System Security Function in Confidentiality

Security function	Description
Identification	The identification function represents the ability to identify the system user attempting to

function	access the system. This function can be completed by a username or a process ID, etc. [40].
Authentication function	After defining the identification of the user, it needs to be authenticated. The authentication function is utilized to check user identity. For example, the user identity can be proved by passwords, iris scans, etc. [41][42].
Authorization function	Authorization determines what a user can do on the system and what are the given permissions to his/her. This function assures that, the user authenticated has the authorization to access areas within the system [43] [11].

- The ***Integrity*** aspect of the CIA triad concerns protection against undesired changes, to protect data from unauthorized modification or intentional corruption [44]. The key system integrity concepts are shown in Table (2).

Table 2: System Security Function in Integrity

Security function	Description
Backup data function	A backup is a copy of the system information on a storage device or an easily accessible external medium for file restoration or archival goals [41]. That allows for data protection and recovery when unexpected or intentional disasters occur [42].
Firewall function	Access and targeted attacks on internet-based systems [41] [42].
Antivirus function	Systems based on data exchange via either public or private networks always require a high level of security to protect data from various intruders. Secure communication channels are provided by applying the public key infrastructure (PKI) approach to external security protocols such as access control services [11][43].

- The ***Availability*** aspect of the CIA triad is related to the ability of authorized users to access information when it is required [23][45]. The key system availability concepts to be defined and measured are shown in Table (3).

Table 3: System Security Function in Availability

Security function	Description
Redundancy function	Redundancy is a technique that provides continuity plans that generally include strategies failure, recovery, and redundancies for essential servers, networks, and data. The network redundancy will automatically turn on into effect to support network availability when the network and server go down [40][41]. While data redundancy ensures that, copies of data are available from the data repository system when needed.
Automatic restart function	Different failures could occur in the system process, resulting in system failure. The corrupted processes can be made to restart by using the automatic restart feature [23].

B. Software security requirements

Software security requirements present the need for a software component's security in its environment, to achieve its tasks accurately, completely, and correctly within the time and this Helps the system ensures software availability and suitability for every task that is performed in the software.

Software security requirements following is internal security requirements (protect within the same software) and external security requirements (protect the software from another software) [22]. The goal of this step is to define the software security requirements that can protect the healthcare software from any threats. This includes internal and external security measures:

1- External security requirements:

- ***Access auditability*** controls the leak of software information or data [22]. The goal of an access audit is to carry out a detailed inspection of software accessibility and services delivered from it. Access auditability function can be achieved by using an audit log. Which are note the user's system access (such as by monitoring who has executed an action, what action was performed, and how the software system reacted. Therefore, access auditability assists developers and testers in several ways: analyzing suspicious activities on the software system, detecting issues, and monitoring software system for possible security breaches or vulnerabilities.
- ***Data corruption prevention*** refers to protect the software system data from both loss and corruption [22]. Data corruption is a common software error that occurs due to data loss or improperly written code. Which happens when the developer reads, writes, transmits, stores, or processing source code. Which leads to software system crashes and hangs. Therefore, the developers should save the source code in offline backups frequently.
- ***Access confidentiality*** refers to protecting the software against illegal access or illegal operation [22]. The healthcare

software system needs to restrict access to healthcare systems by determining security requirements that guarantee access to the system for the intended user and guarantee that the access control policies or constraints specified are enforced correctly. Access confidentiality depends on whether the control is exercised by the ID owner. It concentrates on the specification of access control policies, which is concerned that every access to information or resources is controlled and that only authorized access can take place. This is done by using multiple-access technology for active and passive access control. for example, if the system has used only the password, that does not guarantee the complete confidentiality of the system. Where the user can give the password to another person or hack the password and take illegal actions on the system. In this case, it is difficult to prove who carried out these actions. Active access control ensures more security by using personal identifiers such as the iris fingerprint or the fingerprint. In healthcare systems, it is preferable to use multiple-access technology for high security and prevent any illegal access or operation in the healthcare software system.

2- **Internal security requirements:**

- ***Encryption/decryption*****,** the most popular method of preventing unauthorized data change is encryption. The core of data encryption is to convert data into a non-readable and meaningless text for unauthorized parties. Encrypted text is also called ciphered text. It effectively guarantees the integrity of the data and prevents the data from being tampered with. While the decryption transforms the encrypted data into readable data with the private key [11].

C. Healthcare System Architecture

The lack of security protocols creates a vulnerability, and this leads to misused data or manipulated information, breaches sensitive data and renders a system unreliable or unusable [46] [47]. These critical events could lead to destructive effects on companies, such as damage to the companies' reputation, loss of trust, identity theft, and huge financial losses [48].

The security goal can be achieved at the early phase in analysis phase by analyzing the healthcare system architecture that offers the required functionalities. This helps with early detection and avoidance of security problems. When the healthcare system architecture design reaches the implementation phase, the developer can determine the functional requirements regarding a security method to thwart cyber-attacks [8].

System architecture is a collection of services; these services can communicate with each other to exchange information [49]. When designing a secure healthcare architecture from the beginning, allows the system to handle different security issues such as integrity limitations, high availability, minimizing business risk, keeping confidentiality, etc. E- healthcare architecture is composed of different users, data repositories, and all the health- care systems that exist, as seen in Figure 2. The E-healthcare system architecture enables data communications between users and systems of the whole healthcare system. This section intent to extend a detailed description of the healthcare system architecture.

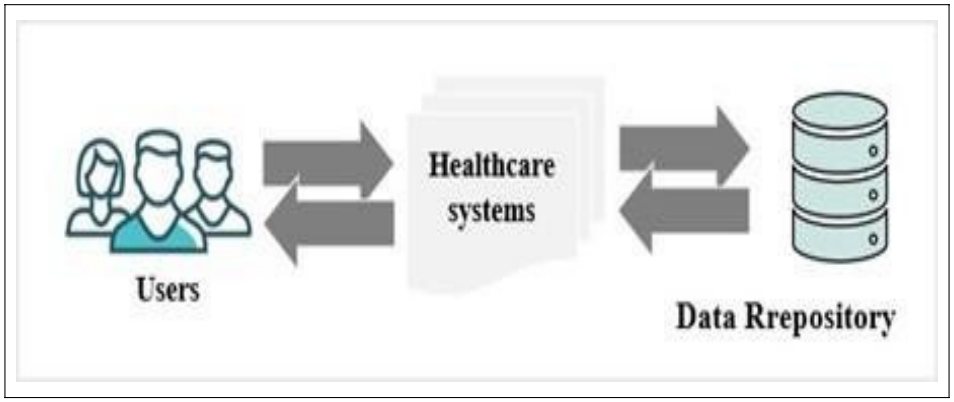

Fig. 2: E-Healthcare Architecture Components

To deploy a secure healthcare system effectively, healthcare systems need clear, consistent, testable, and measurable architecture. The architecture of the healthcare system has been represented based on the Common Software Measurement International Consortium (COSMIC) -ISO 19761 standard [21], as seen in Figure 4, to define security requirements regardless of the languages or type of software. COSMIC is a recognized international standard (ISO/IEC 19761). COSMIC-ISO 19761 is concerned with the data flow between software and hardware. According to this standard. The COSMIC technique allows for four different sorts of data movement: entry (E), exit (X), read (R), and writing (W). The COSMIC model describes the values, guidelines, and procedures for defining the functional size. The functional size can be defined as a gauge of the quantity of functionality offered by the software. To deal with current security challenges, we need a security approach to address various security requirements and manage them. The goal of the COSMIC framework

standard design is to satisfy the requirements of E-healthcare security challenges. To guarantee a system can, find threats. Data movement type in COSMIC-ISO 19761 represents the following:

- ENTRIES and EXITS**:** enabling data exchange with users. The entry represents the sent data. While the exit represents the received data.

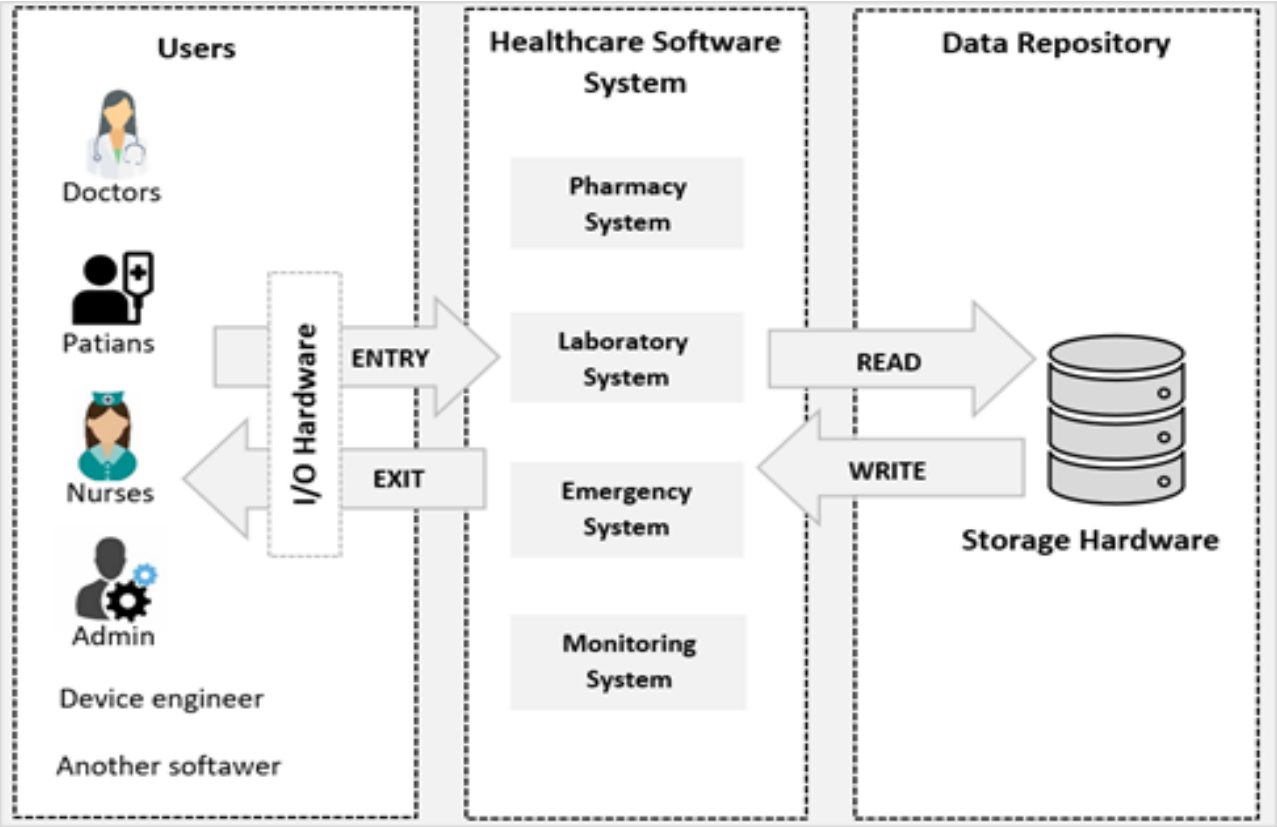

Fig. 3: E-Healthcare Architecture Using COSMIC-ISO 19761 standard repository. Read represents reading data from data storage. While the write represents writing data on data storage.

I/O hardware, such as a keyboard, monitor, printer, or mouse, as well as designed devices like sensors, define the boundaries of software. Also, the software is bounded by data storage hardware like a hard disk, or a Read Only Memory (ROM), or a Random Access Memory (RAM).

1. **User:** E-healthcare contains different users and devices. Various types of users utilize and access healthcare systems, such as doctors, patients, nurses, admins, device engineers, and other software. They interact with the user interface (UI) of the system and request a set of services. Each user has a set of permissions to access the system that differs from one user to another. Doctors have more access powers than the patients. For example, they use the system to create reports, follow up on their patients' condition, prescribe and dispense medications, etc. As for the patients, they have very limited powers. The architecture allows data communications and processing between users and systems which respond to receive users' requests.
2. **Healthcare software systems:** in the healthcare area, there are various systems in hospitals such as laboratory systems, pharmacy systems, emergency systems, monitoring systems, etc. Each system has software that meets user requirements.
3. **Data repository:** the data repository is representing many databases that collect, arrange, and store data sets for data analysis are part of a huge database infrastructure, reporting and sharing. It can furthermore share resources between multiple clients and systems from the data store by reading data from it and receiving written data from the users.

This section shows the architecture of the healthcare system depends on the COSMIC- ISO 19761 standard. Which helps define the amount of security requirements available in the healthcare architecture. This architecture is considered the basis of the standard- based approach for the healthcare security system to address various security requirements and to manage them properly.

4 Designing A Standard-Based Approach for Healthcare Security System

This section presents the designing of the standard-based approach, that used to improve the security of healthcare system, based on the system/software security requirements that were clarified in section 3. These security requirements were defined based on previous academic literature and international standards such as IEEE, ECSS, and ISO standards. These security requirements are applied on the components of the healthcare system architecture described in section 4. The standard-based approach uses the COSMIC modeling to show the function kinds of system and software security requirements in healthcare system architecture.

A. System security requirements

The system security requirements (confidentiality, availability, and integrity) are combined and represented, as shown in Figure 4. This ensures complete protection of the PHI and protection from any threat that may endanger the healthcare system. The CIA requirements used in healthcare system architecture, to guide the development team when building a healthcare system is illustrated as follows:

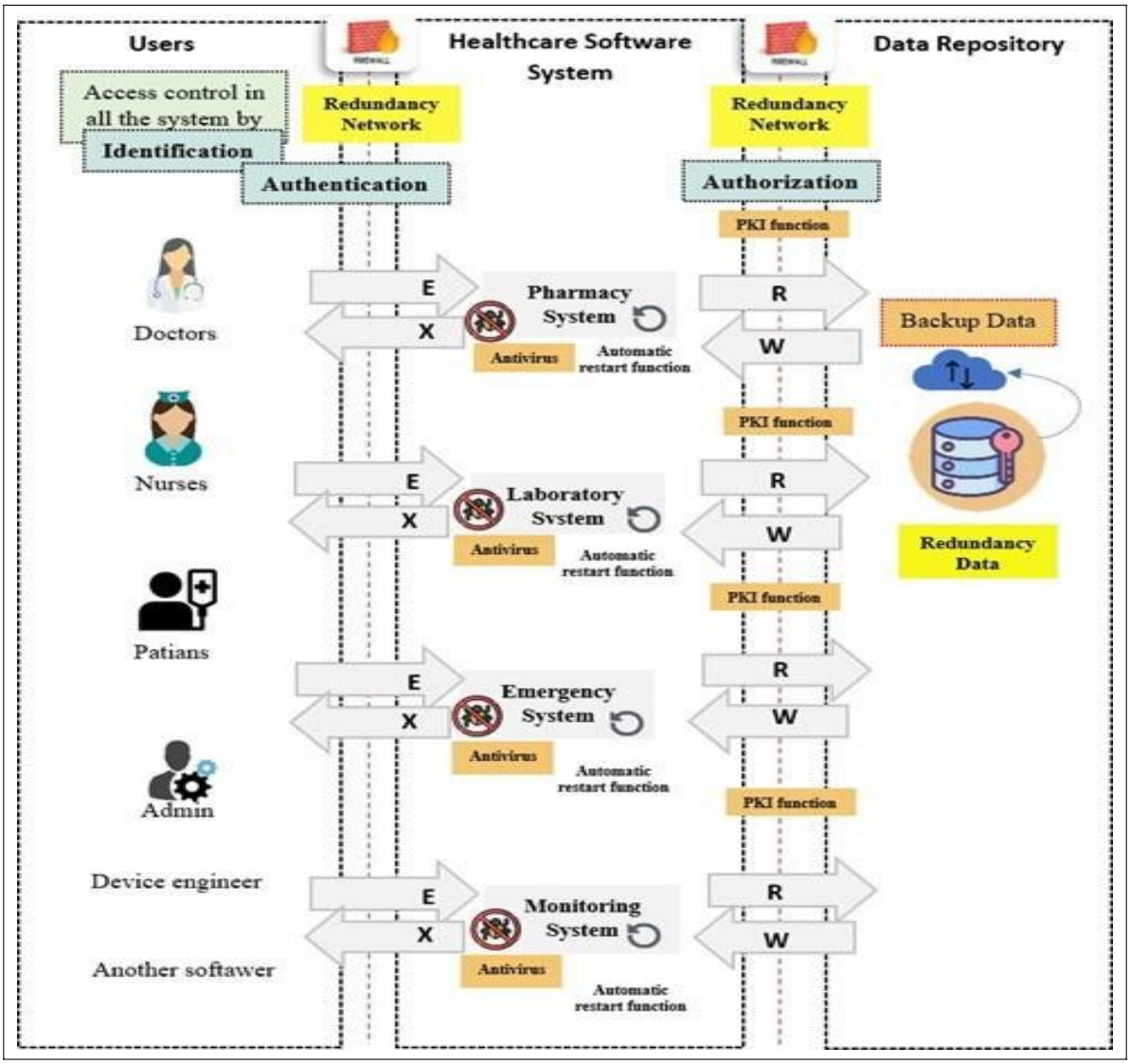

Fig. 4: System Security Functions: COSMIC Modelling View

1. System confidentiality functions

The system confidentiality function is the first function in the system security requirements. To obtain a high degree of confidentiality, the rules on access control should be set by using an *(identification, authentication, and authorization)* function. These three functions have been applied to the healthcare system architecture, as seen in Figure 4. Which shows

that the users should enter an identification function and authentication to verify their user identity and allow them to have access to a particular healthcare system to use the services want. The access control uses data storage for reading their entry data, also for recording their data moves thereon. In turn, the access to services is determined according to the authority of each user to assure the person who has successfully authenticated has been granted access to system areas.

2. System integrity functions

To ensure the data integrity, a set of security requirements is followed as seen in Figure 4. Which shows that *back-up* copies of the data are retrieved from the data repositories and kept offline to save a data copy and preserve them from loss and damage. The *firewall* is used to monitor and control the flow of traffic across the network and to prevent unauthorized access by any user. Also, the *antivirus* is used to prevent any virus or spyware from taking over the system, so the antivirus and firewalls should exist in each device that has a healthcare system. The *PKI* technique is used to control access and provide secure communication channels when sharing data between different healthcare systems.

3. System availability functions

The availability function is considered a critical function because of the sensitivity of the healthcare systems data. Wherefore, the healthcare systems should be ensured available 24 hours a day by following a set of functions, as seen in Figure 4. To ensure the network is always available even when any problem occurs, the healthcare system should be setting *redundancy* for servers and networks. Data redundancy is also used to ensure that data is always available and to guarantee that data can be accessed even in cases of system failure. As for health care systems failure problems, the *automatic restart* is used to force the system to restart.

B. Software security requirements

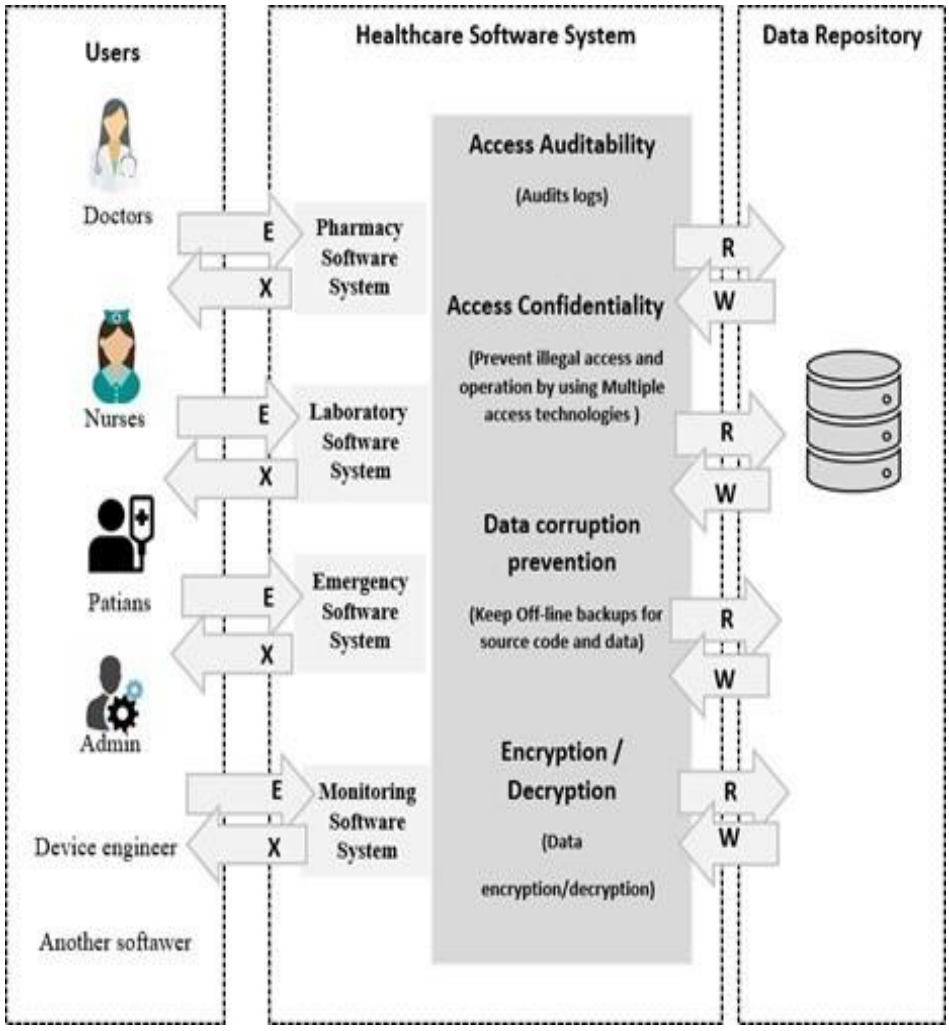

Fig. 5: Software Security Functions: COSMIC Modelling View

The software security requirements are preventative measures taken to ensure that vulnerabilities aren't inserted into the software. The software security requirements should be considered in the early stage, to guarantee the healthcare software system is secured and protected from any tampering or hacking that may occur. The function types of software security requirements required to achieve a high level of healthcare system security are listed below, as shown in Figure 5.

1. **Access auditability,** the healthcare software system should have an audit log to record the information's users have accessed such as: (date, time, the accessing of software frequency, data access, users ID, and the user device type used to access the software. In case of any software hack detected, the organization system immediately takes an appropriate measure accordingly.
2. **Data corruption prevention:** the healthcare entities should always keep the data and source code protected from any corruption by saving it in offline backups.
3. **Access confidentiality,** the healthcare software system should have a preventative measure to restrict and prevent the users from any illegal access or operations by using multiple- access technologies.
4. **Encryption/Decryption,** the healthcare software system should have this mechanism to the sensitive data inside the healthcare software.

5 A Standard-based Approach for Healthcare Security System Based on COSMIC-ISO 19761

Healthcare software systems are considered critical systems, so should have a high level of security, which impacts achieving a high level of confidentiality, integrity, and availability for the healthcare system. The proposed standard-based approach ensures that the security requirements are applied to the whole architecture healthcare system. Which considers the security requirements for the healthcare system, software, and data communication. This standard-based approach can also become a reference approach for improving the security of health care. Figure 6 shows the final standard-based approach for the healthcare security systems after considering both software and system security requirements.

6 Case Study

This section explains an instance of utilizing the proposed standard-based approach for the healthcare security system. In a daily working, each employee, doctor, and nurse use After a patient file is finished, the doctor uses his or her computer to generate or amend it before sending the finished file to the shared central data store. Original document, or a portion of it remains on the user's computer. This puts the healthcare system at risk of being attacked by attackers. For example, malware called ransomware encrypts data and locks down computers until a ransom is paid for it. [50]. When this happens in healthcare systems, sensitive functions are delayed or become ineffective. Failure in patient data can put lives at risk. Hospitals are therefore compelled to resume using the traditional method, i.e., paper and pen, thus sluggish medical procedure, delaying patient care, and slackening medical procedures and tests. For healthcare organizations that have not prepared for such attacks, which restrict access to files and systems, ransomware can be particularly damaging for day-to-day operations. So, every healthcare system should take certain measures to strengthen protection against ransomware by appropriately securing systems, and software.

The ransom can be much higher cost than the security measures. Therefore, to safeguard the healthcare system from this threat; the healthcare entity should adopt a proactive approach. In this example, a set of system/software security requirements is used to protect the pharmacy system in healthcare system from ransomware.

One of the various systems used in pharmacy system, Electronic-prescriptions (E-prescribing) software. This allows to create new prescriptions, track the previous ones, cancel it, or renew them. To keep the pharmacy system protected from any violation, there are a set of security requirements should be applied, it is illustrate below as seen in Figure 7 and Figure 8. Ransomware viruses infect the device in different ways; deceptive emails that have malicious attachments, clicking a malicious link by the user, and displaying an ad that contains malware. This is usually caused by the user's unawareness of how this software penetrates the devices.

C. To solve security challenges, the first step in protecting the system is to implement a suitable strategy for training the users [52]. Therefore, training on the right way it is advised that PHI be used and handled in decrease data breaches generated by employee errors.

D. Restrict access to the pharmacy system only to allowed users, by using an access control method (identification function, authentication, authorization.

E. Protecting from attacks needs an active strategy that focuses on prevention. Malware is especially hard to stop after it has made its way into the computer system. Therefore, it is recommended to use the antivirus and the firewall.

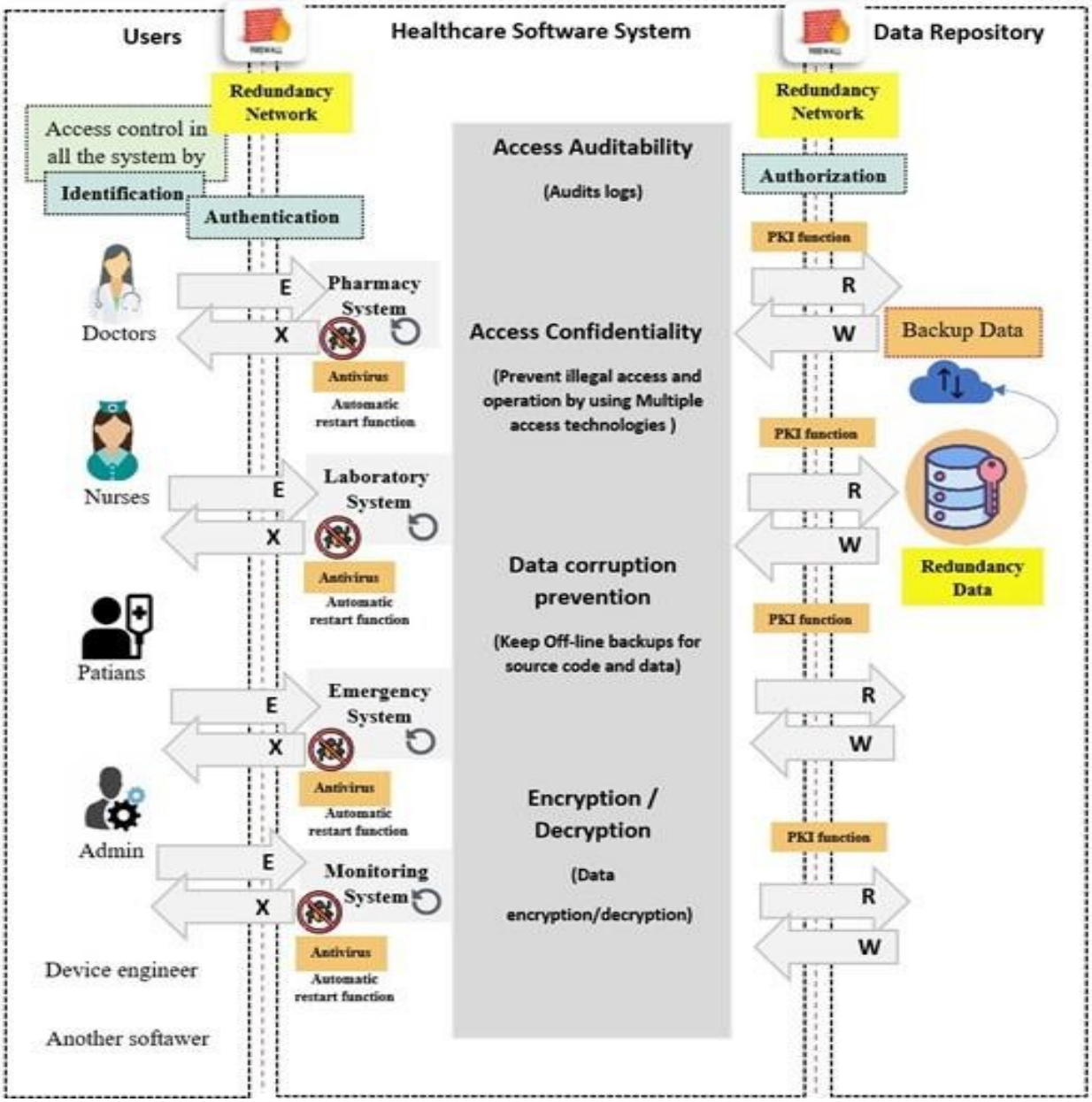

Fig. 6: Standard-Based Approach for Healthcare System Security Requirements

F. Keep back-ups data up to date of prescription files and keep them offline. The thing that makes malware so dangerous is usually the impact on an organization. If the organization stores data in multiple places, it will be easier to handle attack operations, even if attackers have stopped elements in your network.

G. The prescription is an important factor for the treatment of patients, and any deletion or blocking of it by ransomware may harm the health of patients greatly. So, to ensure that data is always available and to guarantee that prescriptions files can be accessed even in cases of system failure should be used data redundancy, by providing a copy of prescriptions from the data repository system when needed.

H. Encryption of the prescription files is the best strategy to prevent access to patient data.

I. Accessing auditability in the healthcare system helps the software detect any access via unauthorized devices. Also, it helps track changes that have been made to the data. Then finds out the source from which this data has been tampered with. It tracks the date and time when the attacker accessed and modified the data; identifies information about the device used the attacker to help find out who was responsible for downloading the ransomware on the healthcare system and to make the employees more careful about their movements.

J. Access confidentiality is important in the healthcare system to monitor the access of users to the software to see if a user performs illegal operations.

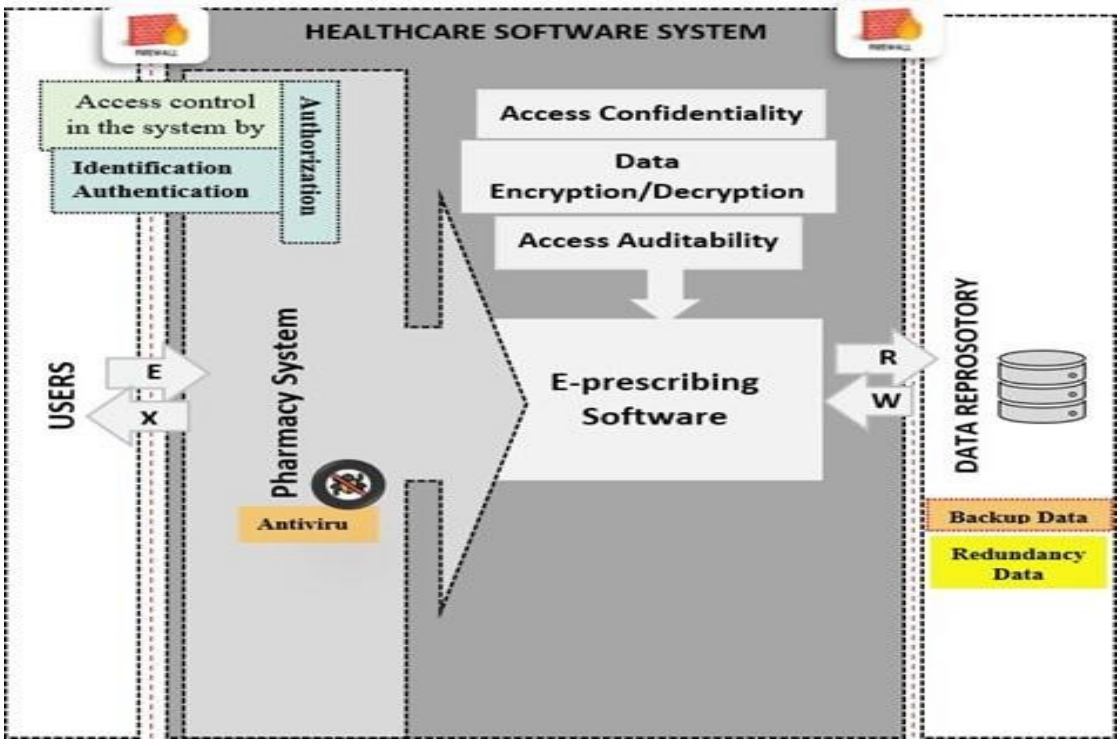

Fig. 7: System and Software Security Requirements to Prevent the Ransomware

1. Conclusion And Further Work

In recent years, the security of data is one of the most obstacles encountered in the healthcare system. Moreover, the healthcare systems have had the highest cost of breaches. The combination of sensitive patient information and vulnerability makes the healthcare system the most attractive target for criminal groups. Therefore, it has become necessary to develop systems that provide full protection for patients and take security requirements into account from the early stages. Security requirements are identified to solve a specific security problem or eliminate a potential vulnerability. Standard security requirements enable developers of security controls to impose specific restrictions on the system functions. Since security is generally defined as NFR, organizations commonly release security fixes after the development has been completed, or when security problems are encountered. This often increases the risk of having some security flaws. Therefore, security issues are ignored in most healthcare systems, and software engineers usually fail to give appropriate attention to security problems. The research work presented in this paper has introduced a new standard-based approach for healthcare system security. For designing this approach, the security requirements are involved in the early phases of system implementation to raise the security of the healthcare systems, by focusing on security from the beginning. This combines security system requirements and security software requirements. The standard-based approach is designed to improve the security in the healthcare architecture, which are designed according to the COSMIC ISO/IEC 19761 standards. This standard-based approach creates an efficient system that aids professionals in the medical field and security management.

In future work, we look forward to making the requirements adaptable to any changes that may occur, and we also look forward to applying them to a real system such as Hakeem. A running example was introduced for the proposed standard-based approach. This example studied one of the most famous threats to the healthcare systems (i.e.), ransomware. In future work, we look forward to applying this proposed approach to all kinds of threats that can occur in the healthcare system. The internal threat validity includes a small case study. Thus, the case study did not cover the whole research paper. Also, the internal threat validity in this research paper may face difficulty in finding similar research which talks about security requirements in healthcare systems. The external validity in this research paper refers to the generalization of the approach. Contrary to construct validity, which describes the relationship between the experiment's underlying theory and the observations. Many standards and methods have been chosen to design this example; by combining international standards security requirements for systems and software to design a reliable and secure approach. We believe that this approach can be simply employed by individuals knowledgeable in security requirements and COSMIC standard. Anyone familiar with

security standards could also utilize and adapt to this approach. More especially, requirement specialists, security engineers, software architects, and people who are working on the development system, specifically healthcare systems, can utilize the proposed standards-based approach. With this method, healthcare organizations can assess their procedures and identify any holes in them. These gaps can then be filled partially or fully, by employing this standard-based approach.

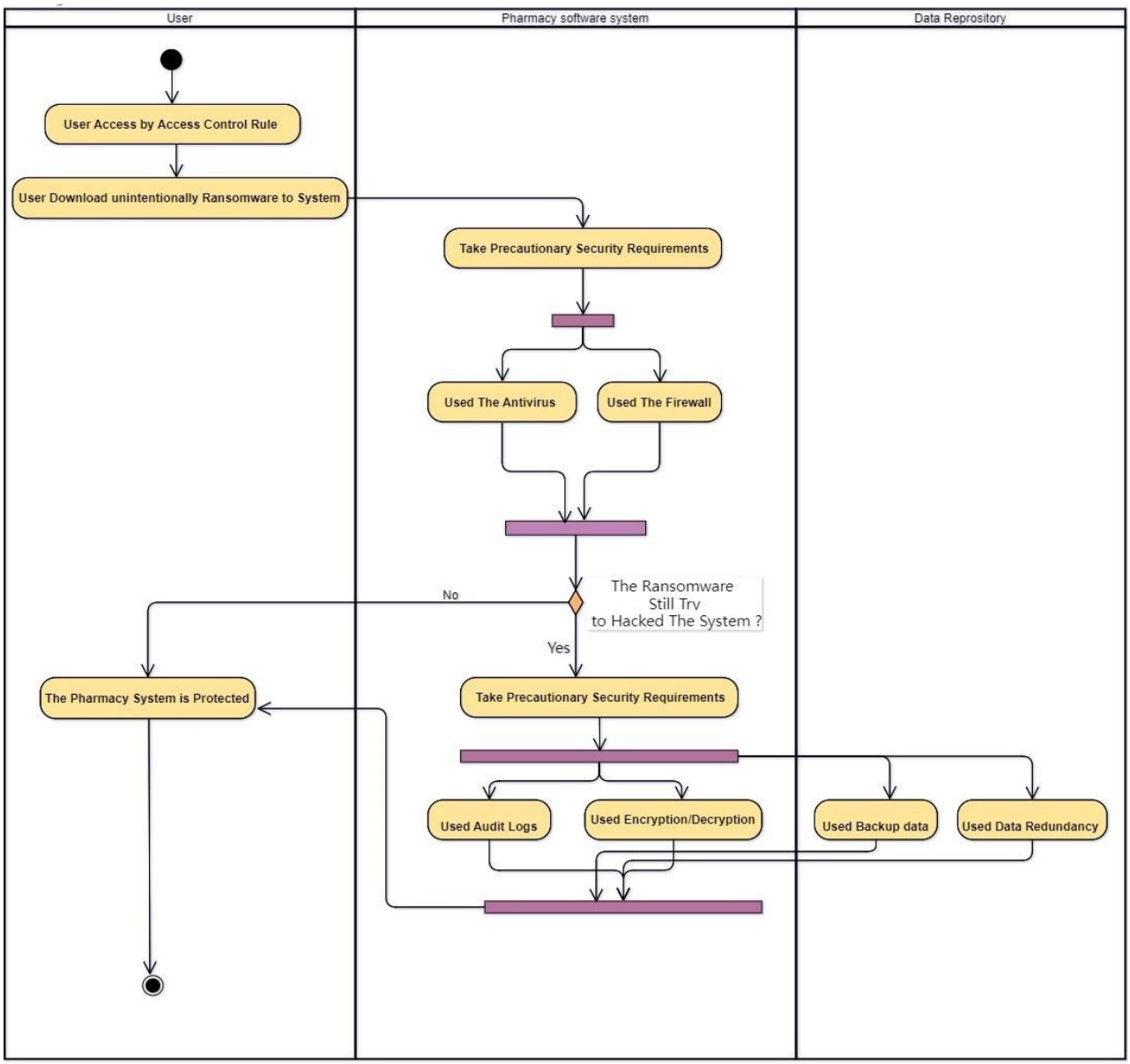

Fig. 9: Security Requirements to Prevent the Ransomware

Conflict of interest

The authors declare that there is no conflict regarding the publication of this paper.

References

[1] S. Moganedi, "Undetectable data breach in iot: Healthcare data at risk," in 17th European Conference on Cyber Warfare and Security, vol. 2 (2018), p. 296.

[2] A. Fatima and R. Colomo-Palacios, "Security aspects in healthcare in- formation systems: A systematic mapping," Procedia computer science **138**, 12–19 (2018).

[3] I. T. Agaku, A. O. Adisa, O. A. Ayo-Yusuf, and G. N. Connolly, "Concern about security and privacy, and perceived

control over collection and use of health information are related to withholding of health information from healthcare providers," J. Am. Med. Informatics Assoc. 21, 374– 378 (2014).

[4] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A sys- tematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," IEEE Access 6, 25167–25177 (2018).

[5] M. Iqbal and R. Matulevic˘ius, "Blockchain as a countermeasure so- lution for security threats of healthcare applications," in *International Conference on Business Process Management,* (Springer, 2021), pp. 67–84.

[6] L. Branch, W. Eller, T. Bias, M. McCawley, D. Myers, B. Gerber, and

[7] J.Bassler, "Trends in malware attacks against united states healthcare organizations, 2016-2017," Glob. Biosecurity **1** (2019).

[8] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and smart healthcare security: a survey," Procedia Comput. Sci. **175**, 615–620 (2020).

[9] S. A. Aljawarneh, A. Alawneh, and R. Jaradat, "Cloud security engineer- ing: Early stages of sdlc," Futur. Gener. Comput. Syst. **74**, 385–392 (2017).

[10] Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering," Comput. Standards & Interfaces **32**, 153–165 (2010).

[11] K. Meridji, K. T. Al-Sarayreh, A. Abran, and S. Trudel, "System security requirements: A framework for early identification, specification and measurement of related software requirements," Comput. Standards & Interfaces **66**, 103346 (2019).

[12] A. Maqousi, T. Balikhina, K. Meridji, and K. T. Al-Sarayreh, "A reference model of security requirements for early identification and measure- ment of security awareness program." J. Theor. & Appl. Inf. Technol. **63** (2014).

[13] IBM. (2021). Cost of a Data Breach Report. https://www.ibm.com/security/data-breach.

[14] A. Hakone, "From spam to medical identity theft: Exploring the vulnera- bilities of electronic medical records," (2015).

[15] N. Sharma, E. A. Oriaku, N. Oriaku *et al.*, "Cost and effects of data breaches, precautions, and disclosure laws," Int. J. Emerg. Trends Soc. Sci. **8**, 33–41 (2020).

[16] M. Begli, F. Derakhshan, and H. Karimipour, "A layered intrusion detec- tion system for critical infrastructure using machine learning," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE),* (IEEE, 2019), pp. 120–124.

[17] ECSS-E-40-Part-1B, (2003) "Space Engineering: Software - Part 1 Principles and Requirements", European Cooperation for Space Standaraization,Netherlands.

[18] ECSS-E-40-Part-2B, (2005) "Space Engineeing:Softwarepart 2 Document Requirements Definitions,." European Cooperation for Space Standaraization,Netherlandss.

[19] IEEE-Std-830, (1998) "IEEE Recommended Practice for Software Requirements Specifications".

[20] ISO/IEC-9126, (2004) "Software Engineering — Product Quality — Part 1: Quality Model 9126–1", International Organization for Standardization, Geneva (Switzerland).

[21] S. J. Ee, Y. H. Tong, A. I. Ibrahim, and F. Zahra, "Secure software development techniques and challenges in their practical application," (2020).

[22] A. Abran and K. T. Al-Sarayreh, "Specification and measurement de- rived from system operations non functional requirements,".

[23] K. T. Al-Sarayreh, M. Alenezi, M. Zarour, and K. Meridji, "A reference measurement framework of software security product quality (spqnfsr)," IET Inf. Secur. **15**, 23–37 (2021).

[24] K. Meridji, K. AlMakhadmeh, K. T. Al-Sarayreh, A. Abuljadayel, andM.Khalaf, "Towards a requirements model of system security using in- ternational standards," Int. journal software engineering its applications 9, 139–164 (2015).

[25] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," IEEE Trans- actions on Softw. Eng. **34**, 133–153 (2008).

[26] N. Nazir, M. K. Nazir *et al.*, "A review of security issues in sdlc," Am. Acad. Sci. Res. J. for Eng. Technol. Sci. **46**,

247–259 (2018).

[27] A. M. Fernandes, A. Pai, and L. M. M. Colaco, "Secure sdlc for iot based health monitor," in *2018 Second International Conference on Electron- ics, Communication and Aerospace Technology (ICECA),* (IEEE, 2018), pp. 1236–1241.

[28] A. Nazir, S. Sholla, and A. Bashir, "An ontology based approach for context-aware security in the internet of things (iot)," Int. J. Wirel. Mi- crow. Technol. (IJWMT) **11**, 28–46 (2021).

[29] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. Ahmad Khan, "Healthcare data breaches: insights and implica- tions," in *Healthcare,* vol. 8 (Multidisciplinary Digital Publishing Institute, 2020), p. 133.

[30] J. X. Jiang and G. Bai, "Evaluation of causes of protected health information breaches," JAMA internal medicine **179**, 265–267 (2019).

[31] H. Hammouchi, O. Cherqi, G. Mezzour, M. Ghogho, and M. El Koutbi, "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time," Procedia Comput. Sci. **151**, 1004–1009 (2019).

[32] S. S. Ambarkar and N. Shekokar, "Toward smart and secure iot based healthcare system," in *Internet of Things, Smart Computing and Tech- nology: A Roadmap Ahead,* (Springer, 2020), pp. 283– 303.

[33] M. Alenezi, "An ontological framework for healthcare web applications security," Int. J. Adv. Comput. Sci. Appl. **12** (2021).

[34] M. Alenezi, An ontological framework for healthcare web.

[35] P. K. D. Pramanik, G. Pareek, and A. Nayyar, "Security and privacy in remote healthcare: Issues, solutions, and standards," in *Telemedicine technologies,* (Elsevier, 2019), pp. 201–225.

[36] J. Adamu, R. Hamzah, and M. M. Rosli, "Security issues and framework of electronic medical record: A review," Bull. Electr. Eng. Informatics **9**, 565–572 (2020).

[37] N. Shrestha, A. Alsadoon, P. Prasad, L. Hourany, and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system," in *2016 Sixth international conference on digital information processing and communications (ICDIPC),* (IEEE, 2016), pp. 75–79.

[38] A. Agrawal, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami, R. Ku- mar, and R. A. Khan, "Evaluating the security impact of healthcare web applications through fuzzy based hybrid approach of multi-criteria decision-making analysis," IEEE Access **8**, 135770–135783 (2020).

[39] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," Egypt. Informatics J. **22**, 177– 183 (2021).

[40] S. Qadir and S. Quadri, "Information availability: An insight into the most important attribute of information security," J. Inf. Secur. **7**, 185– 194 (2016).

[41] S. Saxena and D. Agarwal, "Confidentiality assessment model to esti- mate security during effective e-procurement process," Int. J. Comput. Sci. Issues (IJCSE) **6**, 361–365 (2018).

[42] ISO/IEC 27034-3. (2015). Information technology- Security Application process -- Code of practice for information security controls, International Organization for Standardization – ISO, Geneva.

[43] ECSS (2009b). Space engineering: Software. ECSS-E-ST-40 C. European Cooperation for Space Standardization - ECSS, The Netherlands.

[44] ECSS (2009c). Space engineering: System engineering general requirements. ECSS- E-ST-10 C. European Cooperation for Space Standardization, The Netherlands.

[45] ISO/IEC/IEEE Std 29148. (2011). Systems and software engineering – Life cycle processes – Requirements engineering. (pp. 83): International Organization for Standardization – ISO, Geneva. doi: 10.1109/IEEESTD.2011.6146379.

[46] M. Warkentin and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," Int. J. Inf. Manag. **52**, 102090 (2020).

[47] K. Yee and M. F. Zolkipli, "Review on confidentiality, integrity and availability in information security," J. ICT Educ. **8**, 34–42 (2021).

[48] H. Saleem and M. Naveed, “Sok: Anatomy of data breaches.” Proc. Priv. Enhancing Technol. **2020**, 153–174 (2020).

[49] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, “Survey on threats and attacks on mobile networks,” IEEE Access **4**, 4543–4572 (2016).

[50] T. Rid and B. Buchanan, “Attributing cyber attacks,” J. Strateg. Stud.

[51] **38**, 4–37 (2015).

[52] A. Shaikh, M. Memon, N. Memon, and M. Misbahuddin, “The role of service oriented architecture in telemedicine healthcare system,” in *2009 International Conference on Complex, Intelligent and Software Intensive Systems,* (IEEE, 2009), pp. 208–214.

[53] Mohurle and M. Patil, “A brief study of wannacry threat: Ran- somware attack 2017,” Int. J. Adv. Res. Comput. Sci. **8**, 1938–1940 (2017)

[54] Kasım, Ömer. "An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records." (2022). Fujs, Damjan, Simon Vrhovec, and Damjan Vavpotič. "Towards Personalized User Training for Secure Use of Information Systems." information systems 1 (2022): 14.