JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AUTHENTICATION BASED SECURED INFORMATION ACCESS IN MEDICAL SECTOR: A SURVEY

Abdulrahman Muhammadi[1], Vijayakumar Adaickalam[2]
[1]*Final Year PG Student, Dept of MCA, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru, India*
[2]*Professor, Dept of MCA, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru*
Email: abdulrahmanmuhammadi007@gmail.com[1], vijay.pattukkottai@gmail.com[2]

Abstract: Most people don't take security very seriously in this fast-growing market of the internet, everything is moving online and generating millions and millions of data every second around the world. At the beginning of 2020, the pandemic devastated our lives and all the necessities of our lives become virtual. From our education, shopping, entertainment even healthcare was online. This new norm brought about a lot of breaches, attacks, malicious activities and made the work of hackers and malicious actors very easy. New and improved ways to counter the security issues and differentiate between legitimate users and illegitimate are being implemented, but are not enough. In this survey paper, we review different security measures, access controls, security in different domains of the computer environment, this will have a significant part in the medical field. A deep dive into the world of security for the system that handles millions and millions of people's medical records, its shortcomings, which technologies are being utilized, and what can be done to improve the area of study.

Keywords: **Authentication, Authorization, Biometric factors, Brute force attack, Geolocation factor, Single-factor authentication, Time factor, Two-factor authentication**

1. Introduction

Security is a very general term, which is used daily in some or another way. Most people whenever they hear this word, they think of their physical security such as their property, home, life, and money. Now, technology has advanced so much that physical security and logical security of these aspects of our daily lives are very important. With the invention of mobile and cloud computing, the technology boom has skyrocketed. Everyone wishes to have everything in the palm of their hands. Mobile phones have so much power and computing capabilities, that they can be used as computers. If we compare the strongest personal computer of a decade back with the low-end mobile phone which is currently in the market, the mobile phone will be much faster and stronger. And each of us has become so much dependent on our handheld devices.

Now, what should be done to secure and safeguard the privacy of the people? Promising and providing 100 percent security is always very difficult to accomplish. There always remains a loophole or a vulnerability to be addressed. In the 1970's "cyber security" specifically, security in computer systems was used for the first time and people became aware of it [22]. With the creation of Creepers, a program created by researcher Bob Thomas, it could move freely across the network of ARPANET and leave a trail. From that time till date, many new technology and advancements took place [22].

The 5 Pillars of information assurance is a combination of the CIA Triads, along with authentication and non-Repudiation. CIA is the foundation of the security system of the computer and it summarizes the whole security of the system. CIA means Confidentiality, Integrity, and Availability, whereas, non-repudiation guarantees that no one can dispute transmitting a message with encryption and/or digital electronic signature, or certifying certain data and authentication can be defined as the process of establishing the legitimacy of a user's identification through various security measures [24][29]. Each of these has a critical function to play in the computer system, each of these has its security threats and countermeasures for those security threats.

→ Confidentiality: Every organization whether small or large needs to keep some data of theirs private and confidential. The information or data is so vital for the organization that its survival depends on it. Competitors of the company are always trying to extract that information to get an upper hand in the market. There are different ways and methods to keep that confidential data safe. Some of the methods are; Encryption, Intrusion Detection, Firewall, Penetration testing, and

awareness training and policies. Some of the attacks which can be utilized by the hackers to extract confidential data are; Password attacks, Port scanning, Ping Sweep, Keyloggers, Phishing, and pharming.

→ Integrity: Integrity means that the data in storage or transit should not be changed, manipulated, or deleted by an unauthorized user. If the data or the information is changed, that so-called data is no longer viable and can bring more harm than good. A few techniques that are used for maintaining integrity are Access control, Logging, Monitoring, and auditing are few of the techniques. The attacks that can be used to disrupt the integrity of the data are session hijacking and man-in-the-middle attacks.

→ Availability: Availability of the data or system resource mean the data and the system should be available for utilization to unauthorized users when needed. Most of the time, it's thought that the confidentiality and the integrity of the data are much important. Rather than ensuring the availability of the data, confidentiality and integrity should be safeguarded. It is called as CIA not CI Triads. Ensuring all 3 aspects of the triads are important and availability is very important. Few techniques which are used to ensure the availability of the system are IDS, IPS, and BCPs. Denial of service (DoS), Distributed Denial of service (DDoS), electrical power disruption, and server environment disruption are examples of attacks that can disrupt a system's availability.

→ Non-repudiation: It was more a legal term than a cyber-security terminology back in the 90s. non-repudiation assures that a party receives an email, that has encryption or a message with a digital signature from someone, the receiving party can't deny it. Nonrepudiation validates the data's origin, reliability, and integrity. It verifies the packets which were sent by the sender are properly received and the identity of the sender is also verified based on the description of the receiver. No one can dispute that a communication was sent, read, or digested in this way. It can be attained using cryptography, just like a digital signature. Despite the fact that no security system is flawless, several security experts caution that relying exclusively on a digital signature may not always assure non-repudiation. To achieve non-repudiation, some think that various procedures should be utilized. One such approach is gathering biometrics data and information about the sender that would be hard to refute. It's also worth mentioning that contemporary technological definitions of nonrepudiation only look at the authenticity of the signature. They don't account for the possibility that the signer was coerced, bribed, or tricked into signing. A malware might corrupt a sender's private key, looting or counterfeiting the sender's digital signature and jeopardizing non-repudiation.

→ Authentication: It's the method of validating the user's or system's identity. Authentication confirms the identity of the user when he/she logs in to that system. The fundamental goal of authentication is to enable authorized users access to the system while denying unauthorized users access. The very basic methods of authentication are knowledge-based, inherence-based, and possession-based. Knowledge-based methods consist of knowledge of the authorized user such as usernames and passwords, secret phrases, pin codes, and custom patterns. Inherence-based methods consist of physical features of the authorized user such as fingerprints, face structure, eye retina, and voice match. The possession-based method consists of some third-party device that is independent of the security system such as OTP received on the user's cellphone, smart card, and OTP generator.

These aspects are used in every computer system, data servers, and web servers which are being utilized in different domains. In the medical sector also while setting up all the necessary systems, the CIA Triads are kept in mind in the design and implementation phase. The medical sector is one of the most lucrative sectors, for hackers and malicious actors [17]18]. The reason is the type of data that is being kept in the records of the medical institute namely SSN of the patient, Credit card details of the patients, Insurance details of the patients, and health records of the patients. In most medical institutes still, the primary authentication system is the username and password. There aren't any multiple forms of authentication for the access of the system or access of the data in the medical sector. Physical and Logical security is very much vital for the proper functioning of the medical organization. Physical security, for instance, you can have guards and staff to check the identities of people, measures in case of any emergencies, etc. Apart from the physical security, logical security of the data and information of the medical institute is also very essential. All the information of the patients, the users of the system, the healthcare workers, and the doctors should be stored and accessed safely and securely. In the medical sector, most of the resources and spending are on safeguarding medical records and medical data. How to keep the patients' medical records safe, from the prying eyes of malicious hackers. Safeguarding and securing the system comes secondary. This is because of a few reasons namely: Inadequate spending on the security infrastructure of the healthcare institute, training, and awareness to every user of a particular node that can be used to access the patients' record, and human error. Because of less spending on the security of the systems in healthcare institutes, due to exhaustion and fatigue sometimes the users and the nurses don't remember the proper policy. Which turns out to be a vulnerability and waiting to be exploited by the hackers. For instance, Ransomware attacks are very common within healthcare institutes. Although the management of the healthcare institute pays up, however, 60% of the time the hackers don't keep up their end of the bargain and the cost of recovery for the data is very high. So, keeping all these points in mind there should be created and implemented a new security system which should check the identities of the users of the system and verify their use of the system every time. Such a security system is multi-factor authentication with different security factors for the authentication of the user's identity.

2. Related Work

Fayez Gebali and Mohammad Mamun [1] have suggested a strong, lightweight identification system with a Pass-key exchange model for the Telehealth System for homestay patients to 24/7 keep them under the monitor. They have used a "fuzzy extractor or helper data algorithm" to extract more than one security key for the key exchange. As the paper is based on the IoT system, IOT based security flaws are there. The authors need to address the issue of IoT security flaws in its architecture. Ignacio Velasquez et al. [2] have proposed a framework that lets the software developers choose and contrast the number of authentication systems for their software systems. So, that they can choose and integrate the very best one. The framework itself is best for the job, but it's a little bit tedious for the software developers to do the work manually, cause the proposed system is well known to the author of the system. Maciej Bartlomiejczyk et al. [3] have proposed that mobile is one of the most important parts of our day to day lives, 24/7 it's with us and most of the aspects of our life depends on it. Mobile phones are pocket computers for us. So, ultimately

securing and keeping these devices secure and safe is very much important. In this paper, the author has proposed a system of multi-factor authentication for mobile devices consisting of Knowledge, Possession, Inherence factors for the authentication of the user. The proposed system by the author will help decrease the number of MITM and Replay Attacks in a mobile environment. Sanchari Das et al. [4] tried to address the literature gap which exists in the implementation and design of a multi-factor authentication system. The author proposed that most of the work regarding multi-factor authentication by different researchers is very new. Which has a large literature gap between implementing multi-factor authentication with the systems on hand. Adil Hussain et al. [5] have proposed that data breaches are a very big nuisance to every industry. They not only create problems for the industry but also for the users of those industries. Like if we take the example of the medical sector, most of the affected people by the data breaches are ordinary people who are part of that medical sector. So, according to the authors, the data of the medical sectors are very much susceptible because they are breached by outsiders as well as insiders. This paper gives us a grim reality for our data and how it's easy for an attacker to hack our data and infiltrate our privacy. Aaron Henricks and Houssain Kettani [6] proposed the shortcomings of the MFA system itself. Usually, the MFA system is a combination of 2 or more factors and these factors are used interchangeably. According to the research done by the author, mostly the organizations are still stuck with usernames and passwords which is not enough in this electronic era. To safeguard and keep our privacy safe and sound we need to keep a very keen eye on our security. And try to integrate new security systems into our day-to-day lives. And multi-factor authentication is one of them. Muath Obaidat et al. [7] have proposed the following main contributions which can be summarized as follows: i) It proposed a new paradigm for multi-factor authentication without the limitations of the literature gap which existed in the MFA systems. ii) The technique that the author has used in the proposed system, incorporated a combination of hybrid layered encryption schemes for a dynamic 2FA verification system. iii) The proposed system doesn't add unnecessary work to the user. iv) The system is very fast, in terms of processing. v) And the system is technically sound against the brute-force attack. Vinod Kumar Mahor et al. [8] have addressed in their paper that "we speak a lot about securing our system, laptops, desktops mobile phones but usually, these devices ask for services from the servers". And the security of severs are also very much crucial for the proper working of our lives. So, in this paper, the author has proposed an MFA system for the network of servers connected. The author has suggested that in a multi-server scenario, an anonymization technique is used. The protocol has been put to the test against a variety of assaults, including stolen smart card attacks, middle attacks, impersonator attacks, and so on. The system also works well against the Man-in-the-Middle-, and Brute force attacks. S Bezzateev and S Fomicheva [9] proposed a very simple trust level of the user method. Based on the trust level of each user the system authenticates them and gives them access to the data. This system can reduce a lot of corporate data loss due to failure and or unauthorized access of the elements of cyber-physical systems. Mrs. Tamara Saad Mohamed [10] worked on multi-factor authentication and its importance, in terms of data breaches and mitigating unauthorized access in an organization. In this paper, the author has explained various security measures of multi-factor authentication and their key features. Following are the factors which are normally used in an MFA system. i) Knowledge factor; ii) Possession factor; ii) Inherence factor. Cardinali [11] has proposed in his paper that assessment by the healthcare organization is very important, the staff should be well informed and trained, a strong auditing and logging security mechanism should be integrated, and a strong security policy of background checks for the staff. Fatima Kalsoom [12] et al. proposed behavioral biometric access in the medical sector. With the use of different biometric factors, unauthorized access to the data and system in the medical sector can be drastically mitigated. Tahir et al. [13] proposed in their paper the merging of 5G technology with different aspects of the healthcare sector. The role of this new technology will be prominent in the sector such as security, communication, network, and the most important is the merging of 5G and IoT for smart healthcare. The opportunities it will have in the research and technology of new systems in the healthcare sector are eminent. Mihai Scutaru et al. [14] proposed in their paper regarding different security approaches for the networks architecture being utilized in the healthcare sector. Their approach consists of two layers namely the internal layer for unauthorized access and controls the permissions for the users, such as a smartcard token-based authentication system. The second approach is safeguarding the network from outer attacks using traffic filtering, IDPS, and VPN tunneling. Sanjay Deo [16] speaks about the harsh reality of the current situation of the healthcare sector in the United States, especially with the arrival of the pandemic, the number of data breaches and unauthorized access has increased, and each breach costing $7.1 million. According to the author, the best way to safeguard against these attacks is knowledge. The organization should be fully equipped and always ready to fix any vulnerability which exists. The organization should adopt security best practices and the staff should be well trained. The healthcare organization should have a strong Risk assessment program that should be up-to-date and should cover all the vulnerabilities and shortcomings and should be effective in case of any attack happens internally or externally.

3. Analysis: Security systems in a computer

Most of the time a lot of users don't take authentication and authorization seriously while designing their systems. In terms of the medical sector, authentication can play a significant influence in reducing and mitigating several unauthorized access and data breaches [20]. Although, various security measures like encryption and cryptographic algorithms are used at the backend of the system to keep the confidential and private data of the users and patients safe still the malicious attackers get their hands on the data using different means. In 2019 from the start of the pandemic there can be seen a drastic increase in data breaches in the medical sector. The most common and expensive attack is ransomware which costs the Healthcare facility and the government billions of dollars. Most of the researchers have emphasized keeping the data in storage and transit safe from malicious actors, which is important but finding a safe and secure way to access that data is also very important. Because most of the time the system becomes vulnerable due to the unintentional mistakes of the users, lack of training regarding the cyber rules and regulations, and weak security policies. To understand the security in detail we will be looking into each of the aspects one by one.

Authentication is the act of proving the legitimacy of the identity of the user, using different security measures or credentials like username and password, OTP, Face-recognition, Biometric, time, and location. However, authorization is to allow (permissions) the specific user to use the system once his/her identity has been verified. Usually, the authorization is followed by authentication. There are a variety of authentication methods available, ranging between credential access and biometric, to authenticate a user's identity before granting access to the system. These techniques of authentication provide different layers of security and prevent

attacks like data breaches and unauthorized access. However, a mix of several sorts of authentications is frequently used to ensure safe system reinforcement against potential threats.

3.1 Forms of authentications:

Authentication prevents unauthorized users from accessing databases, networks, and other computer resources. For verification and confirmation of user identification, these methods of authentication utilize security precautions (variables). A couple of the authentication mechanisms are listed below [20].

3.1.1 Primary Authentication: The most popular type of authentication, often known as primary authentication, is also the weakest because it only needs one parameter (security measure) to acquire full system access. A login and password, a PIN, or a One-time Password can all be used as a factor. Phishing, keylogging, or guessing are all relatively trivial ways to break single-factor authentication systems. This method is extremely vulnerable to attacks. To make system access a little bit more secure and safe, a strong password policy can be combined with the primary form of authentication.

3.1.2 Two-Factor Authentication (2FA): Two-factor authentication can be defined as adding a second security measure to verify the identity of the user to the already existing primary factor authentication. It acts as a second layer of security; this confirms the user's identity before allowing them to log in to the system. Users must submit their login details (such as the username and password) and then an additional bit of identifying details, such as an OTP or a push message on their mobile devices, in this mode of authentication. The additional factor is typically tougher to crack or hack since it generally necessitates a gadget or something that only the legitimate user has access to and is unconnected to the system. An OTP from an OTP generator app, a cell number, a device that may receive a push notification, a Text message, or biometric factors such as fingerprint, facial recognition, or retina scan are all viable additional factors (safeguards).

3.1.3 Single Sign-On (SSO): Users simply need to log in to one application to receive access to a wide range of other applications or different services of the same application. This method of authentication is easier for users and has been accepted and recognized by many users, as it eliminates the need to have different sets of usernames/passwords for different services of the same websites and it creates a more user-friendly UX. Establishing a centralized domain (preferably, an IAM system) and afterward developing safe and protected SSO linkages across diverse resources might help organizations achieve this. This procedure enables domain-monitored user authentication, ensuring that when legitimate users terminate their session, they securely log out of all associated resources and apps with a single sign-out. Successfully logging out of the given system is usually not a habit for a lot of users, they just close the browser which keeps the session on. The single sign-on method of authentication has increased the risk of "Credential Stuffing Attack". it is a common habit of internet users to keep the same password for different accounts. The attackers take advantage of this habit. If an attacker gets his hand on a credential for a specific website through different means. The attacker uses the same credentials acquired earlier and will try to login into different websites and web applications based on the history of the target to gain access to those sites.

3.1.4 Multi-Factor Authentication (MFA): Multi-factor authentication is presently the best way of authentication since it verifies users using multiple system-independent factors. MFA employs a variety of criteria, including knowledge, possession, and inherence. However, whereas 2FA always uses two factors, MFA might employ three or more, with the possibility to be switched across sessions, introducing an enigmatic aspect for invalid users. This method of user verification always makes the work of the hackers or attackers difficult, because for each session the authenticator may authenticate the user's identity with different security factors.

3.2 Various Authentication Techniques:

Authentication techniques are the standards for communication and validation that devices employ to connect with the server or authenticator. For different applications or systems that users need access to or work with, there are different rules and protocols for them. Following are a few of the very common authentication protocols which are used:

3.2.1 Password Authentication Protocol (PAP): PAP is the most often used and weakest technique for verifying users because of its insufficient or non-existent encryption. It is a simple log-in to the system using a username and password. Now, PAP is used as the very last option while establishing a secure communication channel between the user and the server.

3.2.2 Challenge Handshake Authentication Protocol (CHAP): CHAP is much better as compared to PAP, due to its encryption and its 3-way handshake. First, the Node (endpoint) sends a secret message to the router with the hash value of it. The router sends the response with the hash value back to the node. After the verification of the response, the handshake is established or denied. This is a much more secure and safe authentication method of authentication.

3.2.3 Extensible Authentication Protocol (EAP): This technique allows a variety of authentication methods, from OTP to smart cards. Due to its compatibility, EAP is primarily used in wireless technology. EAP is the most secure wireless protection technique because it enables an access point and a remote device to automatically execute the authentication process with built-in encryption depending on their credentials.

3.3 Types of Authentication Attacks:

3.3.1 Brute force: Using combinations of username and password or OTP for a certain website to guess the right username and password and credentials and to gain access to the website. For this type of attack, the attacker has his/her custom-built piece of software, program, or tool.

3.3.2 Insufficient Authentication: An attacker accesses a website or a web application that doesn't have enough or strong authentication procedures and the attacker can easily access confidential data and information.

3.3.3 Weak Password Recovery Validation: An attacker accesses a website or a web application and illegally changes, modifies, and deletes other users' passwords.

3.3.4 Man-in-the-middle (MITM): When the communication of two parties is being listened to by a third party without the information or knowledge of the two communicating parties.

3.3.5 Impersonation attacks: The attacker poses as a trusted person to steal confidential information or money from the user or an organization.

3.4 Simple Security system

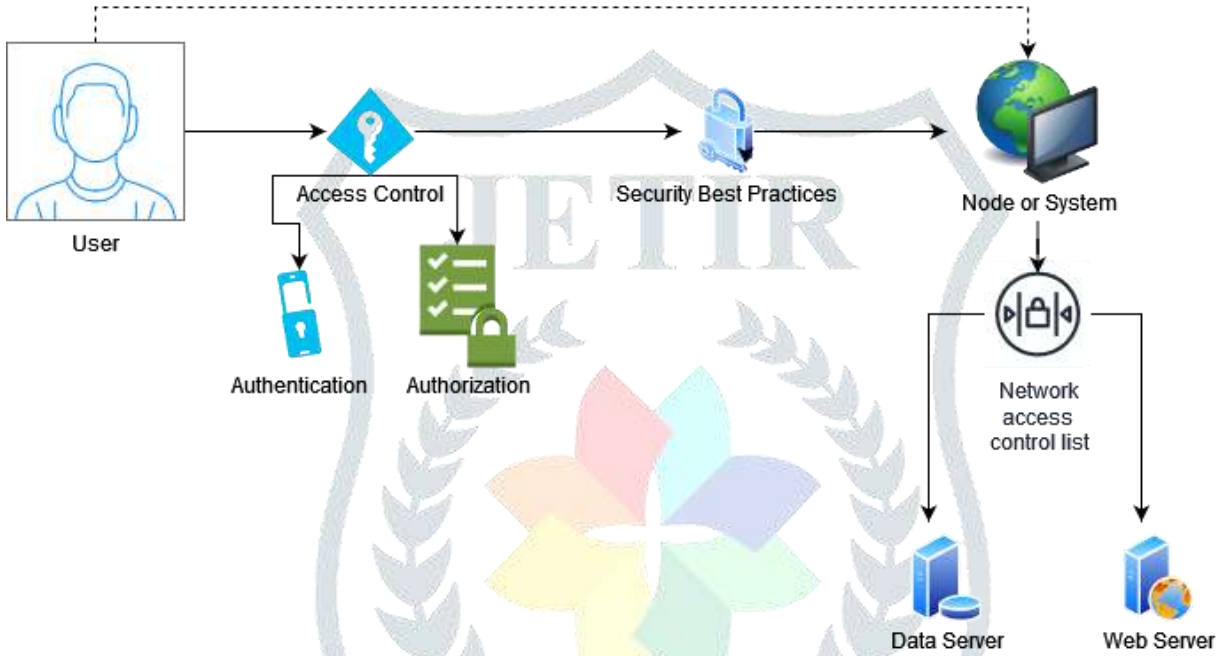

Fig 3.4 Diagram for a simple security system for a computer system

4.1 Analysis: Security in Medical Sector

In today's digitized environment, cybersecurity and data protection are critical for healthcare companies to function normally. Electronic health records, e-prescribing systems, practice administration support systems, and other forms of specialized health information systems are used by many healthcare institutions. Countless devices that make the IoT in a healthcare institution must also be safeguarded, in addition to all of the systems outlined above. Intelligent elevators, sophisticated heating, ventilation, and air conditioning (HVAC) systems, infusion pumps, remote health monitoring equipment, and other technologies fall into this category. These are some examples of electronic gadgets that healthcare organizations require. [27].

4.1.a Block Diagram for cybersecurity in healthcare

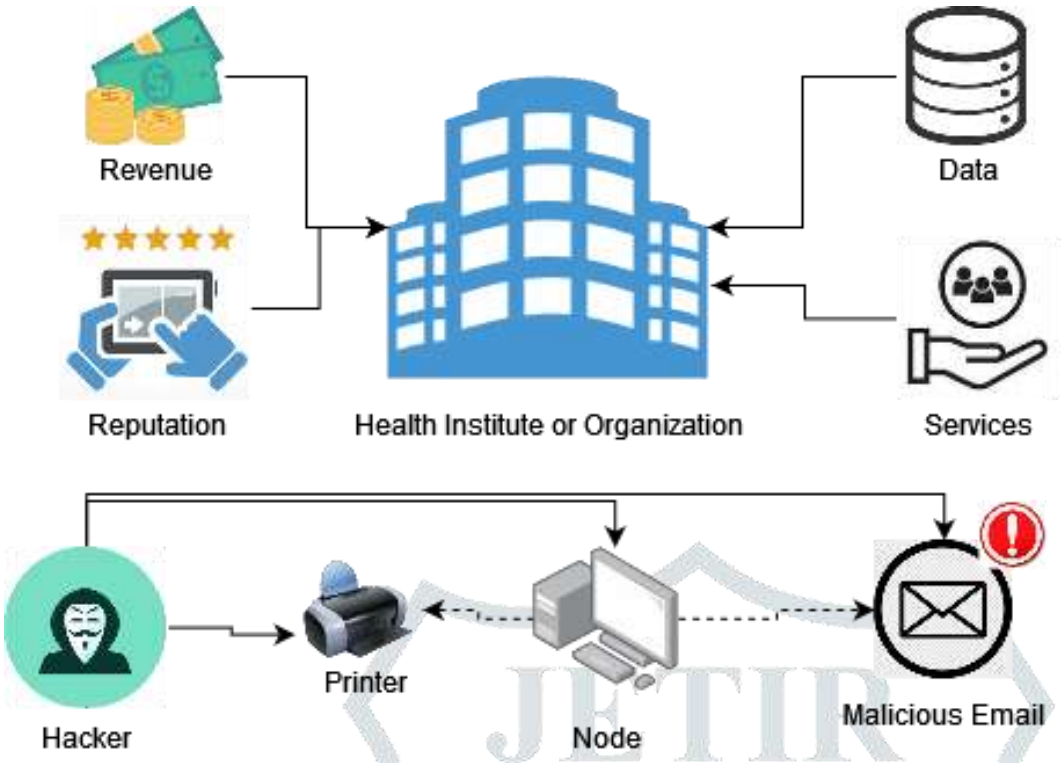

Fig 4.1.a Simple cyber-attack diagram in Healthcare Institute.

4.1.1 Email

Apart from the dedicated system for internal communication email also plays a primary role in communication within healthcare organizations as well as with the other stakeholders of healthcare. Different kind of information is being sent, received, and dispersed using email systems. With time, the size of the mailbox of the email systems grew due to the different types of information regarding the patients being stored and accessed namely credit, insurance, healthcare, and many more [28]. Due to all these reasons keeping an eye on the email security of the healthcare organization has become essential. The phishing attack is very common in healthcare organizations. Unintentionally some staff members may open a malicious email or a malicious attachment that can infect their system. Through the network, the malicious program may infect the rest of the computer systems. Using that phishing email the attacker may steal some important information of the computer, or may install any type of malicious code or program which gives the attacker complete access to that Computer system without the knowledge of the healthcare management.

4.1.2 Physical Security

Physical security of the systems at hand or in the healthcare organization is also very much important. For this purpose, in most healthcare institutes and organizations guards, cameras, and other physical security countermeasures are there. Apart from all these measures employee and staff training and awareness are also very important to be done. For example, the employees shouldn't leave their PCs, Laptops, or cell phones unattended. This itself is a very big security flaw.

4.1.3 Legacy Systems

Legacy systems are still being used in most healthcare institutes because of the cost of the updated system. Healthcare institutes and organizations don't want to spend more money on the device or system which is working perfectly. Legacy systems are such systems that the manufacturers have stopped supporting. They can be software, OS, or healthcare devices running on old OS. There are a lot of legacy systems in different healthcare institutions which pose a big cyber security challenge. Another reason within organizations, old systems may exist is that there may not be any upgrade for them.

4.2 Threats in Medical Sector

4.2.1 Cyber Threats

Ransomware is a serious danger to medical institutions' data confidentiality, integrity, and availability. When ransomware infects a computer or equipment, the files, system resources, and other data are encrypted, and access is limited. [27]. For the data to be released a huge payment is being sought. In basic words, the hacker holds the personal documents, and a demand is made for ransom payment to get the data back. The demand is issued in bitcoins since it cannot be traced. Many distinct forms of malware, in addition to ransomware, represent a threat to healthcare businesses. Namely, credential snatching and wipers.

4.2.2 Phishing attacks

In a phishing attack, the hackers use different electronic mailing systems as means for attack. The attacker would normally disguise himself or herself as a government, official or someone from the organization where the target works, which people normally trust, and send the victim an email known as a phishing email. The body of the email is written so precisely and in a professional manner that it makes the user believe that it's from a legit source without checking the address of the email, and he/she shares confidential information with the attacker.

4.3 Cybersecurity in Healthcare Best Practices

4.3.1 Risk Assessments

Risk assessments are critical for healthcare information security. Prior to taking any action to assist control the risk, it must first be evaluated. Risk must be assessed based on variables such as the likelihood of occurrence, the impact on the organization, and risk prioritization. Risk Assessments should be performed or evaluated on a regular basis, at the very least once a year.

4.3.2 Controls for security

Every healthcare institution should, in theory, have both basic and sophisticated security procedures. This will guarantee that there is a defense-in-depth security system in place, with one control being replaced by another if one fails. A virus, for example, may get past a company's firewall yet be stopped by an anti-virus application [28]. However, not all cyber-attacks and mishaps can be avoided. For healthcare cybersecurity, a solid incident response strategy is required. If any security problems occur, they may be either stopped or dealt with quickly and effectively [23].

4.3.2.1 Basic security controls:

Anti-virus: Your computer is protected by antivirus software against harmful malware and cybercriminals. It analyses data such as websites, webpages, files, software, and apps going across the network to your devices. It searches for known risks that might harm your system and monitors all application activities, notifying users of any unexpected activity. Its purpose is to prevent or eliminate malware. Cloud-based antivirus software, stand-alone antivirus software, and security software suites are all examples of antivirus software.

Backup and restoration of files/data: The data in a medical sector device is always very much essential for the day-to-day activities of the organization and it should be backed up on a daily or weekly basis. Backup is the first step in the restoration of files. For instance, if there is a backup copy of the information in the event of Ransomware, the management of the healthcare organization need not pay a hefty amount to the cybercriminals. They can restore the data from the backup. This instance can be viable only when there is a proper backup system in play, the size of the healthcare organization, and the BCP plan the healthcare organization has implemented.

Data loss prevention: Data loss prevention, often known as DLP, is the process of detecting and stopping security flaws, exfiltration, or unlawful deletion of sensitive data. Businesses employ data loss prevention (DLP) to safeguard and safeguard their information while still conforming to standards.

Email gateway: An email server that secures an organization's or a user's internal email server is known as an email gateway. Every incoming and outgoing email pass via this server, which serves as a gateway. A Secure Email Gateway (SEG) is hardware or piece of software that monitors emails transmitted and received. Email gateway protection is intended to keep spam out of your inbox while still allowing you to send authentic emails. Spam, phishing attacks, viruses, and false content are examples of unwanted messages. Outgoing messages can be analyzed to prohibit confidential material from exiting the organization or to automatically secure emails classified information. SEG capability may be implemented as a cloud service or as on-premises hardware, depending on the organization's needs.

Encryption at rest: This is the encryption of info that has been saved in a storage equipment or a database and is not being transmitted over a network. This gives an extra layer of security and authenticity to the data which is stored in a database. Encryption at rest is a good practice, especially in the medical sector.

Encryption for archived files/data: Encryption for archived files/data is that archived data may be accessed seldom, once in a blue moon. And usually, very important data are archived or retained for a longer period. Encryption of archived data is also very important and critical for the business and people. For example, archived medical information of heads of state and people of power.

Encryption in transit: While the data is sent over the network between organizations and healthcare centers, the data should be encrypted and should be kept safe from different attacks such as Man-in-the-middle.

Firewall: A firewall is a network protection device that detects and restricts network activity as per security standards. There are various types of firewalls such as Packet filter, Connection tracking, Application layer, and Endpoint Specific.

Incident response plan: A successful incident response (IR) plan is a mix of staff, process, and technology that is documented, analysed and trained in the event of a data break. The purpose of the incident response strategy is to avoid data and financial loss while resuming normal routine.

Intrusion detection and prevention system: ID is the process of continually evaluating and analysing occurrences in a computer or network for signs of impending problems, such as violation of cybersecurity legislation, authorized usage standards, or standard safety practices. An intrusion detection system is a software that simplifies the intrusion detection process (IDS). An intrusion prevention system (IPS) is software that combines all of the capabilities of an intrusion detection system with the goal of preventing events. IDS and IPS systems have a lot in common, and administrators may often stop preventative mechanisms in IPS systems to make them operate as IDSs.

Mobile device management: MDM is a software product that allows IT departments and administrators to manage all mobile endpoints, such as smartphones, laptops, tablets, and Internet of Things (IoT) devices. The organization or the employee can own the endpoints, and the MDM solution can be hosted on-premises or in the cloud. An MDM's purpose is to achieve the correct balance between governance, efficiency, and policy adherence.

Policies and procedures: A security policy is a strategy for putting information security ideas and technology into practice in your company. It's simply a business strategy that focuses only on the protection of a company's data. A security policy differs from security processes and procedures in that it provides high-level and explicit guidance on how your firm should safeguard its data, but it does not explain how that should be done. This gives you the freedom to choose whatever security gadgets and tactics are most appropriate for your business and budget. A security policy is technology and vendor-agnostic; its sole purpose is to establish policy, which you may subsequently apply in any way that achieves the defined objectives.

Secure disposal of data: Data that is discarded, whether printed or digitally, depart your secure environment and is no longer protected by any of your protections. For identity thieves, it's a gold mine. As a result, the GLB Act mandates enterprises to dispose of consumer data securely in a secure manner. Physical Data: It's possible to keep a local shredder, but it's generally very slow for the amount of shredding required. A better practical option would be to collect the documents for shredding in a secured container that enables anyone to drop papers in but prevents them from being taken out. This bin should be secured to the structure (e.g., with a cable lock). The trash is emptied regularly by a collection service provided by a secure shredding vendor. Digital Data: A file is not deleted or erased from a hard drive or other storage media when it is removed. It just indicates that the storage area is open for new files. Free software applications can be used to restore files that were previously deleted, even if they have been overwritten by new files.

Security awareness training: Safety training seeks to empower employees with the information they need to protect themselves and their firm's property from loss or injury. In any security awareness training argument, employees, temps, contractors, and anybody else who is permitted to make online transactions for the corporation are all considered members of the organization. Security awareness training is often provided to all workers once or twice a year by organizations that must conform to industry rules or standards such as PCI, HIPAA (Health Insurance Portability and Accountability Act of 1996), Sarbanes-Oxley reporting requirements, NIST, or ISO.

Vulnerability management program/patch management program: The practice of finding, categorizing, resolving, and managing flaws is known as vulnerability management. It's also known as the detection, reporting, prioritization, and reaction to network vulnerabilities. Vulnerability management is no longer a choice for businesses; in fact, various regulatory, audit, and risk management frameworks are requiring it. Continuous vulnerability assessment and remediation is listed as number four on SANS Security Controls' latest framework, stating that it is necessary to "continuously acquire, assess, and act on new information to identify vulnerabilities, rectify, and minimize the window of opportunity for hackers."

4.3.2.2 Advanced security controls:

Anti-theft devices: Any gadget used to prohibit or dissuade the unauthorized theft of valuable objects is considered an anti-theft device. Anything that decreases the likelihood of your automobiles being stolen or broken into, such as a steering wheel locking mechanism or even a car alarm, falls under this category. These anti-theft devices are not only used with personal possession but also are very effective in the medical sector, in case of physical damage or theft to the organization.

Business continuity and disaster recovery plan: A strategy framework for an organization's reaction to natural and man-made disasters is known as business continuity planning. The leadership and management teams work together to develop and implement a plan that meets the organization's sustainability objectives. The nature, scale, and sophistication of a company's activities are evaluated. A broad variety of risk factors that can cause process disruption are evaluated. These risks to business continuity are based on several factors. Disaster recovery is a firm's plan for dealing with an environmental or man-made disaster. The impact of a disaster, such as a huge earthquake, a class 5 hurricane, or a terrorist strike of devastating proportions, is nearly always inevitable due to the sheer magnitude of the threat. In such situations, health and safety come first. From a company viewpoint, backups of data and business plans, as well as the prevention of damage to assets and property, take precedence. The degree of injury can be greatly reduced if an organization's emergency services anticipate the potential of such occurrences while constructing its infrastructure.

Multi-factor authentication: Multi-factor authentication is a multiple-tiered approach to data and application security wherein a system needs a user to give a mixture of multiple mechanisms to authenticate their identity before enabling them to log in. If one credential is revealed, unauthorized users will be unable to match the second authentication requirement, preventing them from accessing the targeted physical region, computer equipment, network, or database.

Penetration testing: A penetration test simulates a cyberattack on a computer system to identify vulnerable security flaws. Penetration testing aids firms in risk management, data breach prevention, and business continuity. In highly regulated industries like banking and healthcare, this testing is critical for maintaining compliance.

Threat intelligence sharing (also called information sharing): Threat intelligence is information gathered on an existing or impending cyber threat that may be shared to aid in the improvement of defenses against that assault. Threat intelligence extends past IP addresses, hashes, and other common threat markers to provide critical information about a threat activity, including indications of compromise (IoC), indicators of attack (IoA), tactics deployed, and, possibly, the enemy's purpose and identity.

Vulnerability scans Vulnerability scanning: is the process of identifying and categorizing exploitable vulnerabilities in connected devices, computer systems, and applications. This is achieved by assessing the same threat areas used by both domestic and foreign malicious attackers to gain unauthorized access to a company's network and assets, such as firewalls, apps, and services delivered either in or out of, to gain unauthorized access to a company's network and assets. To swiftly find and resolve security problems in networks, systems, and applications, scans are compared to a database of known weaknesses.

5. Conclusion

This survey paper gives a brief description regarding the security of a computer system and cybersecurity in the medical sector using different security measures. Starting from the very basic security measure and up to the most complex and high-end security system, which reduces the number of unauthorized accesses that may be intentional and unintentional. Different security mechanisms and measures have been compared. Based on their advantages and disadvantages. Different authentication protocols are used today in different organizations. The medical sector is one of the most lucrative and expensive sectors, in terms of cybercrimes. An extensive study about cyber security issues in the medical sector has been conducted. The medical sector's threats, communication, records, and cyber security best practices. There are a lot of vulnerabilities that exist in the medical sector and the medical sector is a constant target for cybercriminals and hackers. The data which is used in the medical sector is very valuable due to its financial nature and using that data cybercriminals can easily commit financial fraud.

6. Reference

[1] Fayez Gebali, Mohammad Mamun “Multi-factor Authentication Scheme Using Physically Unclonable Functions”, Journal Internet of Things Engineering Cyber-Physical Human System, Vol. 13, 2021;

[2] Ignacio Velásquez, Angélica Caro and Alfonso Rodríguez, “Multifactor Authentication Methods: A Framework for Their Comparison and Selection”, Intech Open Access peer-reviewed, 2019;

[3] Maciej Bartlomiejczyk, Imed el Fray, Miroslaw Kurkowski, “Multifactor authentication protocol in a mobile environment”, Vol 7, pp 157185-157199 2019;

[4] Das, Sanchari & Wang, Bingxing & Tingle, Zachary & Camp, L... Evaluating User Perception of Multi-Factor Authentication: A Systematic Review, 2019;

[5] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan, “Healthcare Data Breaches: Insights and Implications”, Healthcare Basel MDPI, Vol. 8, no 2, 2020;

[6] Aaron Henricks and Houssain Kettani, “On Data Protection Using Multi-Factor Authentication”, The international conference on Information system and system management, pp 1-4, 2019;

[7] Muath Obaidat, Joseph Brown, Suhaib Obeidat, and Majdi Rawasdeh, “A Hybrid Dynamic Encryption Scheme for MFV: A Novel Paradigm for Remote Authentication”, MDPI, Vol. 20, no 15, pp 1-32, 2020;

[8] Vinod Kumar Mahor, R Padmavathi, Santanu Chatterjee, Sanshray Kumar Dewangan and Manish Kumar, “A secure 3 factor-based fully anonymous user authentication protocol for the multi-server environment”, International Journal of Ad Hoc and Ubiquitous Computing, Vol. 34 No. 1, pp 45-60**,** 2020;

[9] S. V. Bezzateev, S. G. Fomicheva, G. A. Zhemelev, "Agent-based ZeroLogon Vulnerability Detection", *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) 2021*, pp. 1-5, 2021;

[10] Mrs. Tamara Saad Mohamed, “SECURITY OF MULTIFACTOR AUTHENTICATION MODEL TO IMPROVE AUTHENTICATION SYSTEMS”, Vol. 4, no 6, 2019;

[11] Cardinali, R. Safeguarding databases. Information Management & Computer Security, 3(1), 30–37. 1995;

[12] Fatima, K., Nawaz, S., & Mehrban, S. (2019). *Biometric Authentication in Health Care Sector: A Survey. International Conference on Innovative Computing (ICIC).* pp 1 – 10, 2019;

[13] Tahir, Mohammad & Yau, Kok-Lim. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. IEEE Access. PP. 1-1. 2019;

[14] Scutaru, Mihai & Ţoev, Radu & Romanca, Mihai & Alexandru, Marian. A new approach for a healthcare network architecture and security. 2009;

[15] Melanie Maynes, One Simple Action you can take to prevent 99.9 percent of Attacks on your accounts, https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ August 2019;

[16] Sanjay Deo, 2020 a Record Year for Data Breaches https://blog.24by7security.com/2020-a-record-year-for-data-breaches June 2021;

[17] Nate Lord, Top 10 Biggest Healthcare Data Breaches of All-time https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time September 2020;

[18] Anuja Vaidya, https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/ 17 February-2021;

[19] How MFA helps prevent common Cyberattacks https://www.onelogin.com/learn/mfa-types-of-cyber-attacks;

[20] Difference between Authorization and Authentication https://byjus.com/gate/difference-between-authentication-and-authorization/

[21] Cybersecurity in Pharmaceutical Industry, https://isacybersecurity.com/cybersecurity-in-the-pharmaceutical-industry/ August 2020;

[22] Vikki Davies, Cyber security, The History of Cybersecurity, https://cybermagazine.com/cyber-security/history-cybersecurity, Oct 2021;

[23] Ivan Dunskiy, "13 Ways to Prevent Data Breaches in Healthcare", Healthcare, https://demigos.com/blog-post/ways-to-prevent-data-breaches-in-healthcare/, June 2021;

[24] Lee Whorter, 3 Foundations of Cyber Security: CIA Triad, WOZ U, https://woz-u.com/blog/the-3-foundational-promises-of-cyber-security-the-cia-triad-explained/, March 2019;

[25] Dean Wiech, Role-based Access Control in Healthcare, Healthcare IT News, https://www.healthcareitnews.com/blog/role-based-access-control-healthcare, August 2013;

[26] Rakesh Soni, Identity Management in Healthcare: Analysing the industry needs, https://www.loginradius.com/blog/start-with-identity/identity-management-healthcare/, November 2020;

[27] HIMSS, Cybersecurity in Healthcare, https://www.himss.org/resources/cybersecurity-healthcare, 2019;

[28] Steven Bowcut, Cybersecurity in Healthcare, Cybersecurity Guide, https://cybersecurityguide.org/industries/healthcare/, February 2019;

[29] Rahul Awati, Non-Repudiation, Identity and Access Management, Search Security, TechTarget, https://www.techtarget.com/searchsecurity/definition/nonrepudiation, August 2021;