Case Study: An overview of Cyber Security Issues and their Mitigation on Cloud in Healthcare

SixRoos

Chandni Acharya

Singirikonda Madhumitha

Mustavi Islam

Santhoshini Sree Bolisetty

Sanmukh Venkat Sai Nekkenti

Sarika Jakkidi

School of Computing and Engineering: University of Missouri – Kansas City

CS5596A Computer Security I: Cryptography

Sravya Chirandas

Date: 28th April 2022

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

Table of Contents

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

Abstract

Cloud Computing or cloud technologies are the emerging paradigms in this current scenario when all the organizations migrate to the cloud for one reason. Cloud resources provide flexibility, scalability, and more accessible infrastructure, enabling agile businesses to grow faster. It also helps organizations handle more significant amounts of data. However, the cloud platform comes with many threats and vulnerabilities. The essential concerns regarding data confidentiality, integrity, authentication, identity management, and data deletion make it difficult for widespread adoption. The research topic for this course work would be getting to know "Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud." This research paper will cover various security threats like insider threats, ransomware or malware attacks, phishing attacks, data breaches, etc. In addition, a few of the remedies are implemented widely to avoid those attacks in the healthcare system. Our main goal is to research how the user data is being tried to protect from illegitimate access by hackers in the cloud while transmitting and encrypting data in healthcare using algorithms like DES, AES, and RSA. This research paper will also cover a few real-time cyber security attacks and essential steps to avoid those kinds of attacks.

Keywords: Healthcare, cybersecurity, ransomware, insider threat, phishing, data breaches RSA, AES, DES, MFA

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

Literature Review

This paper discusses increasing concerns about security threats in healthcare data and devices. Nowadays, the newer connectivity has exposed medical devices and services to the latest vulnerabilities. Healthcare has been an attractive target for cybersecurity attacks. The authors talk about a holistic approach to how cybersecurity has to become an integral part of patient safety by applying changes to human behavior and technology. (Coventry & Branley, 2018)

This article shows a significant rise in ransomware attacks in the health care sector after the Covid 19 pandemic. The cyber-attack on the US health care system proves that the hospitals have been the target of the attackers among all. The continued occurrence of ransomware attacks via phishing underscores the importance of investing in comprehensive, integrated email security solutions and cybersecurity training to ensure that employees are prepared to spot suspicious emails in both the public and private sectors (Cyberattack Almost Shuts Down Health System, Shows Need for Security, 2021)

Challenges and alternative security methods for protecting the privacy of health records on existing systems are described in this study. These cloud-based health record systems are commonly utilized for patient record administration and instant access to patient's health information for doctors during procedures. A new scheme based on DES was proposed for maintaining health records based on problems and various securities in the old system (Dr. S.Pariselvam, 2019)

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

Introduction

Cloud computing is the most recent tech initiative playing a crucial role globally. In this current world scenario where the Covid19 pandemic has made various rounds worldwide, affecting millions of people mentally or physically, the focus among all possible domains is the healthcare domain. There has been a massive spike of information being handled by the healthcare organizations like an enormous amount of patient data, their present or previous comorbidities, covid-related information, vaccination statuses, etc. The massive amount of data that the organization is handling must be vigilant about a few attributes like confidentiality, authenticity, and integrity. Because of cloud computing, the healthcare industries can bring down the storage costs involved and a few other advantages like easier data retrieval and improvement of privacy related to patient information. Healthcare authorities are using the cloud to provide patients with information to be safe and sound. (RansomwareInHealthcare, 2020) . The cost of medical management has been increasing day by day; hence, to maintain all the information of the patients and other medical personnel with less processing time and cost-effectiveness, the cloud is the best option to choose. Patients, healthcare experts, and public officials expect service providers to ensure the privacy of their information. Thus, it is a top priority for service providers to keep their data safe. But this massive usage of cloud storage in the current scenario leads to many cybersecurity concerns around the industry like data insecurity, malware & ransomware attacks, data breaches, phishing attacks, third-party error attacks, etc. (Cloud Computing healthcare, 2019) . Our research paper describes a few cyber security issues and some solutions for the same, and the usage of cryptographic algorithms like RSA, AES, and DES to avoid data insecurities.

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

Cybersecurity issues in Healthcare and solutions

We will discuss a few cybersecurity attacks in the healthcare industry like data insecurity, ransomware attacks, data breaches or thefts, insider attacks, and phishing attacks and discuss some essential solutions or remedies adopted by healthcare organizations.

Malware or ransomware attack:

This attack occurs because malware infected the organization's systems, making the critical processes slow or majorly inoperable, which would work only when a demanded ransom is provided (nowadays, the ransom is asked in cryptocurrency). Ransomware attacks have hit around 34% of healthcare attacks since last year. (RansomwareattacksProtection, 2022) The attackers basically encrypt the accessible files and provide the decryption key only after the ransom is paid. There can be variety of malwares like encryption ransomware, lock screen ransomware, encrypting web servers' ransomwares. The small-scale hospitals are the soft targets for the bad attackers because of the lowest amount of budget being set aside for security. The recent kind of ransomware gangs active and have taken the center stage are Pysa, Astrolocker, Hive, Rangnarok, etc. where Hive ransomware gangs attacks the healthcare industry majorly. (Ransomware gangs, 2021) A few solutions which the organization can take to avoid the high impact of these attacks could be:

- The hospital data should be backed up and stored in some safe offline storage or on a different network that would be safe from the hackers.
- -Since the hospital data or patient data is susceptible, it should be encrypted, which would make it difficult for criminals to decryption.
- The hospitals are using a multi-factor authentication approach to secure remote access to the email system.

- The devices being used should be placed under a specific VPN, adding the next level of protection, and keeping them in a designated firewall only providing access to listed external IPs. (Ransomware and HIPAA, n.d.)

Data breaches and insecurities:

Data breaches occur very frequently in healthcare. These could occur for various reasons, like some insiders who could accidentally or knowingly disclose the patient information, credential-stealing virus, any lost electronic devices, etc. This kind of breach is widespread because of the PHI or the Personal health information available in the medical databases on the cloud, which are a primary target of cybercriminals. As per various reports, now, around 15 million health records have been compromised through data breaches. After the Covid-19 outbreak, the HIPAA (Health Insurance Portability and Accountability Act) reports suggesting that there has been a 25% increase in the number of data breaches since the year 2020. The major reasons for the rise in breaches were the home healthcare facilities, quicker digitalization, remote workforce, and compromised vendors. (Heathcare Breach report, n.d.)

One of the most important ways or remedies to avoid data insecurity, breaches, and malware or ransomware attacks is data encryption.

Patient Data Encryption:

For data security purposes, the information put on the cloud is in an encrypted form. The DES algorithm was used initially by healthcare providers to resolve the security challenges and avoid data breaches. In this scheme, different healthcare providers provide information about the same patient. Those data indexes are encrypted using DES and can be merged using the cloud without disturbing patients' privacy. It renders efficient and secure query processing with a single data

query submitted by the provider. The cloud from all related providers will process encrypted data without knowing its question (Dr. S.Pariselvam, 2019)

- **Data Providers:** Information providers are mainly those authorities like physicians, hospitals, lab reporters, etc., who provide patient data. The Information provider signs up for an account by giving their details, and they get to log in with their unique username and password. They get access to log in if the password and username match. Then, they can upload information to the cloud. Before uploading them to the cloud, it must be made sure that all the files are encrypted. For every file, index reports are set. Users can view their files in an encrypted format after they upload them. They can log out after submitting the index report. (Dr. S.Pariselvam, 2019)
- **Data Owner**: Patients are the data owners. If they do not have an account, they must create one. After that, people must log in using a login and server. After that, they can log in if the information is correct. Then, the files that have been posted can be viewed and even downloaded by the data owners. To download files, users must submit a request to the cloud server, which the cloud server accepts and provides the file key to the user's email address, where they may then download the file. Owners of personal data can upload files that will be encrypted and kept on a cloud server. The data owner can also see index reports
- in a similar data report. Cloud Server can log in to the site with user details. Cloud can view the data owner and data provider details. All are encrypted using DES. Cloud Server Administrator can view owner details. Cloud Server can accept the requests and sends the file key to the user mail id (Dr. S.Pariselvam, 2019)

  - But this kind of encryption technique does not provide enough security as the cipher key length is 56 bit which lets the attackers get into the system within 24 hours. The DES algorithm is also very much vulnerable to Brute force attacks. (DES, n.d.)

In recent times, healthcare providers are using different encryption techniques like AES or RSA to follow the HIPAA regulations act. As per the HIPAA regulations, healthcare providers need to use encryption methods to protect patients' ePHI records. An encryption key that helps decrypt information avoids unauthorized access to the patient's ePHI. (Ransomware and HIPAA, n.d.)

- **Private key encryption:** In this kind of encryption technique, a particular list of users who can access the encrypted information is permitted by a private key. The key is used to implement an asymmetric AES algorithm (256 bits is the most widely used) where the sender needs the private key to transmit a secured message, and the receiver needs to have a key to decrypt the message. This type of encryption is used for hard drives or databases containing PHIs and the algorithm with the secret key. One way it is easier for usage by the hospital employees is because they don't have the extra burden of remembering more than one key. For example, this technique applies when one employee needs to transfer information to a second employee regarding a particular patient. But the drawback of this kind of encryption algorithm is that since many users have access to the secret key, keeping that information secure would be a tedious task. (Blume, 2016)
- **Public Key Encryption**: In this kind of encryption, the public key allows an authority to access encrypted information, whereas a secret key or private key is needed to decrypt. This is used in RSA encryption which is an asymmetric key algorithm. The usage of this algorithm is for securing sensitive hospital data while being transmitted from the organization's web browser to a web server using HTTP, for example. The

employees in the hospital having the public key could be assured that the information which is being accessed is from a specific entity and the employees receive their secret keys, making it easy for the healthcare providers to identify the recipient. This process of encryption and decryption is better for the healthcare domain as deciphering the information using the exact and correct secret key is difficult. (Blume, 2016)

- To make the encryption of the data work properly, hashing technique is used, which makes sure that there is no tampering done with the encrypted patient information. This technique reveals any changes or alterations to the original data by condensing the information as plain text. (Blume, 2016) . Along with encryption, the hospital should avoid the "Bring your device strategy" as much as possible because that helps to increase user convenience and creates loopholes in the system, making it easier for data breaches. (DataSecurityImprovments, 2019)

Insider Threat:

- Insider threat is any type of malicious activity from users against the organization. This activity is done through legitimate access to the organization's network, databases, or applications. These users can be current employees, former employees, or third parties who have been given access to the organization (partners, contractors, or temporary workers). Insider threats can be classified into three categories which include 1) Malicious Insider, 2) Negligent insider 3) Compromised insider.
- **Malicious Insider:** Malicious insider is someone who knowingly looks to steal information and disrupt operations. Some of the signs of this activity can be identified through a few activities like accessing unique resources, logging in to the health care system or network at unusual times, and transferring too much data through a network.

- **Negligent Insider:** A Negligent insider is someone who unknowingly damages the system and accidentally exposes sensitive data due to not following IT procedures. It occurs when an employee leaves a device disclosed or accidentally clicks on an in-secure link and gets into the trap of malware injection into that system. Many healthcare executives might not be aware of IT security, and hence there are chances that they mishandle physical devices, which may lead to the attacks.
- **Compromised Insider:** A compromised insider is someone whose credentials are unknowingly compromised by an external threat to steal data. Training employees on recognizing and reporting any insider threat can minimize this effect. (Understanding Insider Threats, 2021)

The insider threat is the most dangerous compared to all the others, as the threat actor has legitimate access to the organization's systems and data. Health care is one of the only industries where insiders are responsible for a higher percentage of breaches than external attackers. Insiders cause more significant damage than outsiders as they have easy access to an organization's database. They can have access to sensitive files, and this critical information like financial data, proprietary information, and patient data, when kept in the wrong hands or lost, can cause damaging consequences. Notably, the detection time in the health care and pharmaceutical sector is 350 days, which is remarkably high and results in higher recovery costs, up to 10.8 million dollars annually. (data breachesdue to Insiders, 2018) Hence, the Health care sector area needs much attention. According to Verizon, Insider threats affected 50 percent of the health care organizations. (Insider threats after pandemic, 2020)

Few preventions or remedies which are being adapted for insider threats by organizations are:

- A combination of training employees, organizational alignment, and technology is the right approach for preventing insider attacks. One of the most straightforward approaches is adopting the UEBA approach for tracking, collecting, and analyzing user behavior (Assessing Insider threats, 2020)
- The advanced way of ensuring cyber safety from insider attacks is implementing the EKRAN system, an employee monitoring tool. EKRAN system is being adapted by AGEL (European Health care provider) to enhance the security of sensitive information without changing the system management procedures. Through this practice, monitoring user activity can quickly block suspicious activities (European Healthcare Provider AGEL Protects Sensitive Data from Insider Threats Using Ekran System)
- Adopting ZERO TRUST SECURITY approach which is a network security model based on the idea that no one or device, within or outside an organization's network, should be allowed to connect to organization's IT systems or services unless they have been authenticated and continually checked.

Phishing Attacks:

Phishing attacks here in the healthcare industry typically see one of two objectives: obtaining access to PHI or spreading malware. In this underground economy, PHI has become a desirable resource since it could be used to construct fictitious identities, acquire free medical care, and perform financial crimes. According to a survey report, phishing has been engaged in 59 percent of significant security incidents throughout all organizations and 69 percent of attacks at hospitals. In such situations, the perpetrators were always terrible actors (phishingattacks, 2021) .

Different phishing approaches:

- **Email phishing:** Phishing via emails is the most popular method of attack. One can be prepared to open a document, phone a false support line, or visit a web address in a spam email. There is indeed a sense of urgency in these communications. (health tech magazine, 2020)
- **Fake websites:** Phishing emails are commonly combined with fake websites. A mail would refer directly to a bogus website, which will request personal credentials or banking details once people tap upon that. In some instances, clicking here on a URL may lead your system to get compromised with computer viruses (health tech magazine, 2020) .
- **Fake texts:** Smishing is another term describing simulated text attacks. They are comparable to spam emails. They will disclose this information or contact information, together with a text that leaves you feeling rushed (health tech magazine, 2020)

Remedies used for such attacks are:

- Acknowledge common phishing email Strategies and Techniques: Evaluating the suspect's objectives and strategies is the first way to safeguard an organization from spoofing. As per the Cybersecurity & Infrastructure Security Agency's (CISA) website, A hacker exploits social interaction (social intelligence) to acquire or breach an organization's information or its application servers in an injection attack (Healthit Security, 2021).
- Regular employee cybersecurity training: CISOs can help us understand existing phishing development programs while using the Phish Gauge to analyze click counts and collect feedback from customers on why they clicked on various fake emails since they are designed for the desired population of interest. In addition, organizations must provide individuals with hacking and cyber health tools and education in maintaining

corporate security. Within the coming decades, a successful phishing education campaign might save organizations massive amounts of money while protecting medical confidentiality. (Healthit Security, 2021)

- Staying updated with sector guidance and threat alerts. Best practices in cybersecurity are always changing, just as the systems they safeguard. The FBI, CISA, HC3, and other important organizations and agencies often issue danger briefs and sector alerts to keep businesses informed about cybersecurity threats. NIST regularly provides recommended practices to assist organizations in preventing and responding to phishing and ransomware threats (Healthit Security, 2021)
- Implement Multifactor Authentication. Healthcare firms that haven't yet established 2-step verification or multifactor authentication to protect credentials, should be doing it right away. This can also be achieved by asking people to sign in using a unique, recognized device, thus leaving phishing identities worthless and decreasing the chance that cybercriminals would continue to approach the corporation. (Healthit Security, 2021)
- Implement Multifactor Authentication. Healthcare firms that haven't yet established 2-step verification or multifactor authentication to protect credentials, should be doing it right away. This can also be achieved by asking people to sign in using a unique, recognized device, thus leaving phishing identities worthless and decreasing the chance that cybercriminals would continue to approach the corporation. (phishing attacks, 2021)

Recent Cyber security attacks in healthcare and use of remedies to recover

Healthcare System: An overview of Cyber Security Issues and their Mitigation on Cloud

This section focuses on few of the recent cybersecurity attacks in the healthcare industry and the techniques which they applied to recover from those attacks.

- According to Healthcare IT reports, a medical e-health provider CompuGroup Medical was down of what was mentioned as a technical failure by **a ransomware or malware attack** on December 2021 where the email and phone services were disrupted. Due to the use of various prevention or mitigation solutions like offline back up infrastructure, encryption techniques being used for PHI and the defined response plan for email systems helped to restore key components impacted by the attack within 5 days without hampering the data integrity of the patients' information. (healthcarecyberattacks, 2021)
- A **phishing attack** incident in July 2021 on Mongolia Health systems which reported to US department of Health and Human Services around 4ook people's information being affected which included lot of patient information, health insurance plan numbers, health provider names, patient names, etc. . This information was compromised using the email system of the Mon Health. There were no funds being transferred by the attackers because of existing security protocols but they have been trying to avoid any such cybercrimes in future by engaging in enhancement of security practices like multi factor authentication of email system. (healthcarecyberattacks, 2021)
- A **Ransomware attack** took place in Ophthalmology clinic at Singapore on 16th August 2021 where attackers targeted on the clinic server and clinic management system which included patient's medical records and information about serious illness and treatments of about 7300 patients. This incident is not highlighted in the news until the clinic published in the press release. The Clinic's IT system is not connected to MOH's IT System such as National Electronic Health Record, and hence it did not affect the MOH's IT system. This incident

sounded alarm bells to other clinics. MOH had adopted some healthcare cyber security guidelines in August 2021 to remind all licenses and implementing measures to adopt best practices to promote confidentiality, integrity of IT systems. (IOTW: Medical data, 2021)

- As of late**,** a Kentucky medical care supplier, Park DuValle Community Health Center in Louisville, paid programmers $70,000 in bitcoin to open the clinical records of around 20,000 patients after a ransomware assault secured its framework for almost two months, as indicated by news accounts there. Districts additionally have been the objectives of ongoing ransomware assaults, including Baltimore, Atlanta and Greenville, North Carolina. The Baltimore assailants requested $76,000 in bitcoin emancipate, which the city would not pay; the city as of late proposed involving $10 million in overabundance incomes to pay for the expenses of recuperation, as per the Baltimore Sun. A ransomware assaults a year prior on Blue Springs Family Care in Blue Springs, Missouri, impacted almost 45,000 patients. The clinical practice didn't pay a payoff and had the option to recapture admittance to its framework by utilizing reinforcements, as per a representative. (CynergisTek, 2019)
- Ransomware assaults multiplied in the midst of the pandemic when medical clinics expanded their utilization of remote work and made more emergency clinic information internet, as per a July 21 report by network safety counseling firm. In 2020, 560 medical care associations were casualties of ransomware assaults, the report said. Ransomware assaults cost medical services associations a $20.8 billion in personal time , twofold the sum it cost in 2019, as per a Comparitech report referred to by CynergisTek. A different IBM report observed information breaks in the medical care industry cost a normal of $9.23 million. The expense of ransomware installments has placed a colossal strain on emergency clinic spending plans. Philanthropic

emergency clinics and wellbeing frameworks have been particularly impacted by the expenses of persevering cyberattacks. (Dan Margolies, 2019)

- Another data breach attack happened in Eskenazi Health of Indianapolis, Indiana, a division of Hospital and Health of Marion County in August 2021 where the heath security team had reported that the cyber criminals caught hold of the network using a malicious IP address. Although some patient information was leaked on the dark web, the security team took required steps like taking the whole network offline to protect the sensitive information and there was no ransom that was paid to the attackers. (EskenaziHealth, 2021)
- One of the latest Hive **ransomware attacks** happened in PHC (Partnership healthcare plan of California) where CA based non-profit managed healthcare plan faced a cyberattack which suspended IT systems for more than a week in March 2022. The ransomware gang claimed to have 850000 unique records of names, SSN, addresses, date of births, etc. which were exfiltrated from PHC website which was worth of 400 GB of data. The PHC till date does not confirm any plan members' data being affected. (Ransomware gangs, 2021)
- **Insider attack-** McGraw, a hospital guard built a botnet using the hospital network at Dallas Hospital. For public viewing, he recorded what he called his "botnet infiltration" on video and audio. McGraw installed or transmitted a software on the computers he used that allowed him, or anybody with his user name and password, to access the systems remotely. He also impaired the integrity of certain computer systems by disabling security elements, such as anti-virus software, making the computers and connected network more vulnerable to attack. He also downloaded malicious software (commonly known as "bots") on the majority of the PCs. (Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison, March 18, 2011)

Conclusion

The healthcare industry has been and always will be the most vulnerable to cybersecurity attacks in the coming years because of the sensitive patient information they deal with in everyday basis. As per the reports, the healthcare cybersecurity attacks like ransomware or phishing or insider attacks have increased to around 45 million in 2021 than 34 million in 2020 due to the unprecedented arrival of Covid19 but there are more proactive approaches being taken up currently by the not only the organizations but also about the third-party vendors who have access to the data and networks. The use of some strict approaches has made sure that the cybersecurity attacks slightly dropped during second part of 2021.

References

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and way forward. *Maturitas, International Journal of Midlife health and beyond*.

Daniel, A., & Momoh, M. (2022). A Computer Security System for Cloud Computing Based on Encryption Technique. *Comengapp.unsri.ac.id*.

Dr. S.Pariselvam, M. (2019). Encrypted Cloud Based Personal Health Record Management Using DES Scheme. *IEEE Xplore*.

Kannan, M., Priya, D., & VaishnaviSree, S. (2019). A comparative Analysis of DES, AES and RSA crypti algorithms for network security in cloud computing. *JETIR March* .

Nicholas, K., WIson, C., & Kibe, A. M. (2017). Enhancing trust in cloud computing using MD5 hashing algorithm and RSA encryption standard. *International Journal of Scientific and Engineering Research,Volume 8*.

Pansotra, A., & Singh, S. P. (n.d.). Cloud Security Algorithms. *International Journal of Security and its Applications*.