International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 4193 – 4199

Healthcare Data Security on Cloud Computing During COVID-19 Pandemic

Rajesh Yadav
Research Scholar
SET-MUST, Lakshmangarh
yadav.rajesh27@gmail.com

Dr. Anand Sharma
Asst. professor
SET-MUST, Laxmangarh
anand_glee@yahoo.co.in

Abstract

The development of IT and its formation as an almost pervasive phase of our lives has been one of the important phases of the technology revolution. Now IT is energetic and it's helped in economic and social development of the country. The healthcare industry also improved the services using the information technology. Now information technology is having an important part of healthcare sector. Uses of cloud give a gear in healthcare industry. In COVID-19 pandemic many health organizations has switch on cloud or plan to switch earliest. These crises totally change the medical industry frameworks. In this industry most of areas the e-health concept take place. With increases of cloud in this field also gives invitations to cyber-criminal. It's open a wide opportunity for cyber-crime. They take advantages of unawareness and not more knowledge by health providers. In this paper discuss about the applications which use for treatment and care of patients and also manages the health industry data. Also there discuss about threats which affect the health organizations data and its breaches. And in the last suggest some solutions and suggestions for healthcare organizations to improve the cloud security.

Keywords: *COVID-19, healthcare, cloud, threats, security, cyber-crime.*

1. Introduction

The involvement of cloud in healthcare services that industry leads the finance, energy and utility sectors. Now day's healthcare institutions, hospitals health service agencies are digitalized and brought their information on the cloud. This initial cloud implementation is a big advantage to fight against the pandemic as it expands the capability to analyze the relevant data and take right action. Cloud reduces the IT costs and also avoids the training; purchasing new equipment's and reduces space for hardware and IT people. Also, the cloud cares the telemedicine. Remotely access the information and through interactive tools its helps to take right decisions to doctors and health workers. In healthcare industry the Telehealth is more useful for the doctors who try to evade personally interacting with patients. It's more helpful for diagnosing certain types of conditions also for the processing of healthcare claims.

These features also create information technology a possible target for cyber-attacks. Today, as the world struggles with an exceptional pandemic in the form of Covid-19, continuously

ISSN: 2233-7857 IJFGCN

the hackers are trying to take benefits of the quick changes across industry. In that healthcare industry is most targeted sector for the hackers.

The social distancing becomes necessary at this time so everyone is doing work from home. This remote process they uses the all IT infrastructure remotely. They use association tools for team interaction, accessing data on endpoint devices and so on. These things give opportunity to hackers break the bridge and do the maximum losses.

The Covid-19 eruption has cruelly troubled the business continuity of the medical industry. That creates the situation also for doctors to adapt work from home for all non-coronavirus patients. So this sudden change in the pattern of treatment creates a lot of challenges for doctors and patients also.Hackers always targeting healthcare organizations with phishing battles, ransomware, malicious acts that affect the healthcare data, medical solutions and patients secure information's.

Recently implemented or enhanced medical systems, equipment and IoT based devices connected to medical facility networks may enhanced the organizations attack outward.

2. Tools and Applications to fight against COVID-19

Many Healthcare organizations, Digital health purveyors and Governments try to develop tools and techniques for tracking and preventing the covid-19 cases. As such we know that using a cloud for developing any application is very simple, low cost and secure. So the following mentions applications are developed using cloud computing [1].

- The telemedicine company Fruit Street Health launched a platform (COVID-first virtual care) there covid-19 patients can video consult with doctors. It's also use for new risk assessment.
- The tool CovidMD is built by Salesforce Service Cloud. That offers an automated health's communication. Patients go to the webpage and fill out all entries like their health record and present symptoms, and from there offer personalized guidance and also there opportunity to take telemedicine appointment.
- The tool called Pear-004, there patients with schizophrenia can use the tool for communal skill training, cerebral interactive treatment for neurosis and for disease self-management training. This will be done under a doctor direction.
- A new telemedicine app MediOrbis develop for chronic disease patients in driven by COVID-19. That care long-lasting disease management for situations like diabetes, hypertension and COPD, and it's provided discussions or second view for more complex medical concerns.
- Medical Realities has launched aCovid med edonline resource to train healthcare professionals in vital, benign for COVID-19. There feature contain present COVID-19 guidelines, evaluations of updated pandemic data and related test on the key medical zones.
- Lab Test Company Quest Diagnostics develop antibody test done by online platform (Dubbed Quest Direct). Once the request is started it's sent to doctor, then patient can go there and get their blood sample, and get result online portal.

- The mobile based app COVIDSafe helps health executives to rapidly interaction persons who may have been uncovered to COVID-19. Executives can use the information to alert those who may need to quarantine or get tested.
- The digital health company CarePredict developed a contract-tracing tool PinPoint for oldest living amenities that can be used to way COVID-19. That tool used for four types of tracing: location, path contact and room traffic tracing.
- Danish government implemented COVIDmeter app which allow users to input and monitor the coronavirus symptoms, and app tracks the spread of the virus.
- In Italy Limbix make a headset for healthcare professional for reducing the stress and nervousness to support staff working long shifts for treating patients suffering from coronavirus.
- The Mumbai based healthcare company (AI startup Qure.ai) developed advanced diagnostic software that explanation of COVID-19 propagation from chest X-ray.
- The kingdom of Bahrain launched a GPS chasing electronic bracelets and coronavirus contact tracing application. That app alerts the monitoring places when a patient leaves isolation or misplaces its bracelets and its connection. It's also send picture request to which self-isolation must reply with a photo.
- Flywire and AI-powered are developed a COVID-19 chatbot that gives information to patients about virus and for healthcare workers can help access CCVID-19 risk in patients.
- Siri has given symptom based guidance and also links of telehealth-app for users seeking COVID-19.
- The MobileSmith developed two apps for COVID-19, one for medical supervise and other for public members. The medical staff can use for supervise distribution and video allusions. The public app assistances for assessments. It's also gives information about COVID-19.
- Indian goverment launched an app Arogyasethu for COVID-19 patients attacking. This app also alert to a user if any COVID-19 patients come nearby.
- The cloud based application (Athenhealth) is serving its clients test and screen their patients for COVID-19. There implement diagnostic-testing orders and screening questions to hospital persons.
- DRDO has developed an app (SAMPARC) to track patients who are under quarantine. That app has been used by many state governments of India. This technology is server side application that checks on whether or not patients affected by COVID-19 are quarantine rules. The app only needs the location of patient and their photos.
- Bangalore Medical College and research Institute (BMRCI) is developed an app that store medical history of COVID-19 patients. The app can be used by doctors and senior consultant at warrior control room. That helps to less doctors will affect by virus through patients. This app is design to ensure that there is no delay in treatment of patients [2].

3. Data Security and Cyber-attacks

Healthcare organizations first priority gives care to their patients. For that they don't have too much infrastructure for security to cybercriminals, because there more concerned to spend in

new equipment's, resources, staff training and workers, which is more physical perceptibly communicate to patient care. So cloud is the best choice for healthcare organizations because clouds provide updated infrastructures, new software and services and low cost maintenance and all. Cloud also worry about organizations security of data and all but still its required to work for that[3].

A learning from IBM and Ponemon institute, the budget of healthcare data rose form $380 per breached in 2017 and it increased $408 in 2018 [4].That is the highest cost of data breaches across all industries. Healthcare professionals easily identify the viruses in patients but that's not easy to know in computer. So that can be possible through cybersecurity, its cure the technology, databases, and networks that assist uninterrupted and perfect patient care.

Cyber-attacks interrupt healthcare professional proficiencies. They obstruct the skill to distribute patient data correctly to other healthcare care professional, which is the main feature of digitalization. For an example, a Missouri healthcare was target to a ransomware attack, important to send ambulances as a security measure. The clinic was specialized in trauma and stokes patients [5]. The cyber-attack destroys the entire EHR system that affects the patient care. A Montana hospital had 7,000 patient data was stolen from an employee's e-mail while the worker was trailing outside the country for business [6].The attack was accrued when using the unsecure network.

So that healthcare organizations need a strong security that is companionable for entire organizations without confining innovative efforts around accurate medicine, strength and transparency.

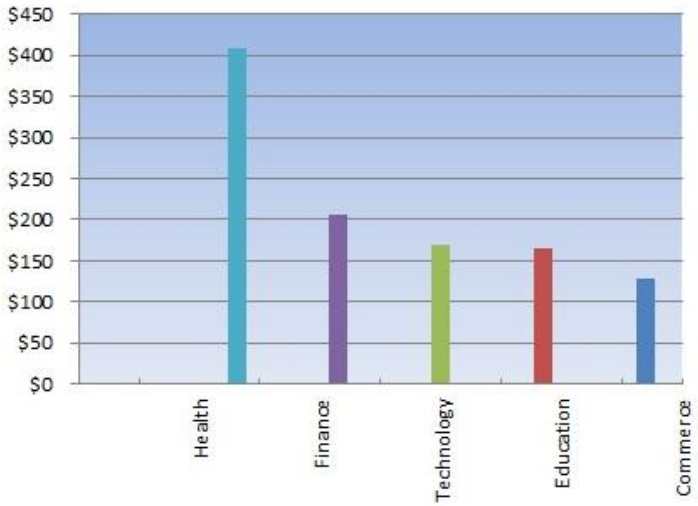

Fig1. Data Breach Cost per Record

4. Cyber Threats to Healthcare Organization

As we know that many most healthcare organizations use the cloud for enhancing our e-health services. Organizations continuously affected by many threats. Unawareness and

technologies breaches affect the healthcare and patients sensitive data. The most common threats in the cloud to the healthcare organizations are described in this section.

A. **Phishing:**

Phishing is a technique there the receiver received the mail by their coworker but reality is that mail is sent by attacker and attaches a URL or file in the mail. When click to open the link or file that ask some sensitive information and infect the computer. Opening the file or URL may malicious software transferred in the computer and stole the important information [7].For an example a medical employee receives a fake e-mail form attacker that instructs to change the password of billing software. When employee click the URL is divert to a bogus login page, which collect the employee's login authentication and spreads this to the attackers. Then the attacker use that information to access the patient data and organizations important information.

B. **Ransomware Attack:**

It's a type of malicious software that functionality is different from other malware. It's denied access to a user's information and encrypt the data, the ransomware direct the user to pay for opening a file. That's no guaranty after payment file will decrypted by hacker. For an example through an e-mail user is directed to a fake website and cheated by downloading a security update. That security update is really a malicious software the locked the data and instruct the user to pay a ransome to unlock the file.

C. **Unintentional or intentional data breach:**

An unintentional insider threat is happened unintentional damage initiated by mistakenly, like misled, technical mistake or negligence of work.

An intentional threats is happened by employee, contractor or any other person of the organization, with a purpose of personal benefits, imposing damage to the organization or any single person. For an example a staff member of outside the hospital collect the patient's data for verification and misuse that patient data for unwanted task.

D. **Attack on medical devices that affect patient safety:**

Now a day's lots of medical devices are implanted for patient's diagnosis, alleviation, treatment or deterrence of disease. A cyber attacker inserts through network and controls the devices. For an example while scanning the attacker takes control and can do power off or reboot the machine again and again and all.

E. **Theft or loss of medical equipment or medical data:**

The loss of devices a big gain of the hackers. If the lost device was not properly protected may result unauthorized or illegitimate access, diffusion and use of complex information. Also if the device is recovered then also data has been lost. The loss of data is compromised the business and patient safety.

F. **Distributed Denial of Service Attack:**

When network is overloaded then it denies the users request and restricts to access the authorized users. Attackers hit on the network and deny to all users request and that's very critical for healthcare to immediate required patient's data for treatment.

5. Security measures during COVID-19

It's alarming situation against cyber-attacks on healthcare industry in COVID-19 crises. Now for healthcare organizations and hospitals must take precautions to protect healthcare equipment's, networks and applications and patient's data from cyber-attacks [8].

- **Secure Network:** its common practices for everyone to use the public or insecure Wi-Fi networks, but it's very serious threat to security. So every healthcare professional required to use only secured network. Also for secure work only use the VPN.
- **Increase Awareness:** the medical professional and hospital employee are not more technically strong. So for healthcare professionals to raise consciousness to avoid data breaches [8].
- **Secure Software:** It's must to use the antivirus software's on all the devices used by healthcare professionals. Also important that only authorized files download on that devices that reduce the chance of installing malware.
- **Device Maintenance:** Computers and laptops must be updated. It's also important to download only required software and applications on those systems. Avoid using portable devices for accessing sensitive data.
- **Required Information's to Access:** Patient information is the liability for hospital. So only authorized persons can access the sensitive data and everyone having permission to access the required data.
- **Data Encryption:** To protecting the hospital information and patient's data, always use the encryption methodology on data. If mistakenly data is hacked by hacker it's not use by them. For that only use the good encrypted tools and software's.

6. Recommendations for Healthcare Organizations

To reduce the cybersecurity risk to healthcare organizations, the following best practices for users and administrators are:

- It's important to ensure that all default passwords must be changed with strong passwords.
- Emphasize the security consciousness ethics and cybersecurity best practices for email, password security, safely use the internet and immediately report the unwanted things on own account.
- Use the multi-level or multi-factor authentication on the application.
- Disable all unnecessary services, ports and applications.
- Time to time updated all hardware and software and tries to use latest infrastructure and software's.

- Deploy on all points the anti-malware software's.
- Put limited access permission according to level and requirements.
- Regularly monitor the all systems, networks and activity done by users.
- Always concern about the data backups and generate multiple copies of data on different places.
- Gives training to our organization people and aware about the threats.

7. Conclusion

The cloud computing allows IT companies to secure patient information and confirm controlling compliance while permitting healthcare providers to continue delivering advanced technological care to cover patient involvement to digital space. The healthcare organization is week to cyber-attacks just other like industry. The increasing cyber security threats to this industry can be condensed significantly by taking defensive measure. In COVID-19 crises required for healthcare organization chooses the best services on cloud for our applications and also update those applications time to time for reduce the risk. It's also very important to gives training and awareness to healthcare providers. That helps to make secure the patients and organizations sensitive data.

References

1. HIMSS Media, "Tech's role in tracking, testing, treating COVID-19" mobihealthnews. May, 1 2020, https://www.mobihealthnews.com/news/roundup-techs-role-tracking-testing-treating-covid-19.
2. Tanu Kulkarni, " BMRCI has an app to track case history of COVID-19 Patients" April, 14 2020, https://www.thehindu.com/news/national/karnataka/bmrci-has-an-app-to-track-case-history-of-covid-19-patients/article31342051.ece.
3. Rajesh yadav, Dr. Anand Sharma, "CLOUD COMPUTING: DATA SECURITY ASPECT" International Journal of Latest Trends in Engineering and Technology Special Issue IC3NS 2018, pp. 014-018.
4. Landi, Heather. "Healthcare Data Breach Costs Remain Highest at $408 Per Record." HealthcareInformatics. Last modified July 13, 2018. https://www.healthcare-informatics.com/news-item/cybersecurity/healthcare-data-breach-costs-remain-highest-408-record.
5. Security Intelligence Staff. "IBM X-Force Threat Intelligence Index 2017." SecurityIntelligence. Last modifiedMarch 29, 2017. https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/.
6. Spitzer, Julie. "Montana Hospital Employee's Email Hacked While Traveling, 8.4K Patients' Data Stolen."Becker's Health IT & CIO Report. Last modified July 17, 2018. https://www.beckershospitalreview.com/cybersecurity/montana-hospital-employee-s-email hacked-while-traveling-8-4k-patients-data-stolen.html,
7. Rose, Scott, Stephen Nightingale, Simson Garfinkel, and Ramaswamy Chandramouli. Trustworthy Email (NIST Special Publication 800-177 Revision 1,Gaithersburg, MD, 2017). https://csrc.nist.gov/CSRC/media/Publications/sp/800-177/rev-1/draft/documents/sp800- 177r1-draft2.pdf.
8. Susan Alexandra, "Cybersecurity & Healthcare During COVID-19", April, 13 2020, https://www.globalsign.com/en/blog/cybersecurity-healthcare-during-covid-19.