WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Emerging trends in Medical Biotechnology & Healthcare through Cyber Security – Cyber-Biosecurity

Probahee Das

MCA at Amity University Noida
Email ID: - Prorisa1313@gmail.com

ABSTRACT

The expanding digitization of the biological sciences places higher value on the data generated, information gathered and knowledge gained. Failing to secure data will affect a company or country's competency to place itself optimally in the approaching fourth industrial insurgence . The equipment and service providers that run physical exploration and expansion are also each connected online. Failing to shield these resources from intrusion increases the threat of incidental or calculated detriment, for illustration by the loss of control over biological yields. Cyber-biosecurity is arising multidisciplinary field that combines cybersecurity, biosecurity, and cyber-physical security as relates to natural systems. To better distinguish the perceived troubles at the interface between cybersecurity and biosecurity, Biosecure conducted a pilot study that surveyed the opinions of a separate party of foreign field leaders in biotechnology . Crucial findings of the inspection showed that cyber-biosecurity threats were considered to be delicate to characterize due to variations in types of dangers, targets and implicit impacts, and accelerated by a eminent variation between the position of complication or maturity of mitigation and response measures.

INTRODUCTION

The outbreak of the Covid-19 pandemic last year started a surge of cyber-attacks in the life sciences industry, and the trouble is likely to get worse.**[1]**. Biotech startups need to ameliorate their cybersecurity, but where should they start? Cyber-attackers range from lone individualities to government-patronized associations and strike in a variety of ways, similar to nipping data or sabotaging companies. What's certain is that cyber-attacks on life sciences and healthcare associations are enhancing amidst the universal Covid-19 pandemic. **[2]** .One factor is that biotech holdings went through the roof last year as the pandemic pelted the industry into the limelight. As they make it easier than ever to collect, cache, and assay hereditary data, they also make the data appealing to would-be cybercriminals.**[3]**

Objective of Study :-

Importance of Patient Health and Data :-

In healthcare, the patient's health and their privacy is a top priority, and it is increasingly reliant on medical devices and systems. Patients got admitted in Hospital with the hope of being treated well but nowadays a lot cases like money laundering or security breaches or data stolen etc can be heard . Cyber-attacks on Protected Health Information (PHI), Personal Identification Information (PII), and other programs also make patient as well as doctors and medical attendees life miserable day by day. Loss of access to medical devices and records, similar to a ransomware attack, can encrypt and hold files hostage. The hacker can access a patient's private data and they can use for blackmailing or sell it on dark web. Also, the attacker can intentionally or unintentionally alter the patient data, leading to serious damage to patient health.**[11]**

This Research shows my concern and suggestion to prevent Cyber Crime in the Medical Industry, because this is the most vulnerable industry among all other fields. Most of the Cyber Crime cases mainly in India are from Hospitals or pharmacy .

How is Medical Biotechnology advancing modern healthcare & medicine?

Medical biotechnology is the use of living cells and cell materials to probe and produce medicinal and diagnostic products that help treat and avert human diseases. Biotechnology is generally used to ameliorate medicine due to the advantages and pieces of knowledge it provides similar to understanding the inheritable composition of the human species, foundational structure of genetic disorder manipulation and, repairing of damaged genes to cure conditions. It provides effective diagnostics, forestallment and, treatment measures including the production of novel medicaments and recombinant vaccines. It's a toolbox loaded with numerous kinds of living cells and their component molecules and numerous ways to use them.**[12]**

Tissue Nano transfection: new science may have the competency to heal people with a single touch. Tissue Nano transfection works by injecting inheritable code into skin cells, which turns those skin cells into the other types of cells needed for treating diseases. In some lab tests, one touch of TNT fully repaired the injured legs of mice over countable weeks by turning skin cells into vascular cells. And purportedly, this bio-tech will work on different kinds of tissue besides skin. The capability for this type of gene remedy is huge, from helping automobile crash victims to active duty warriors. Medical biotechnology has made this advancement possible, and the continued exploration and testing will simply help ameliorate this tech and embrace it across hospitals and medical centers.**[11] [12]**

Recombinant DNA technology is combining DNA molecules from two distinct species and also inserting that new DNA into a host organism. That host organism will produce new genetic combinations as per drug, husbandry, and industrial needs. There are numerous exemplifications of recombinant DNA technology being used, from biopharmaceuticals and diagnostics to energy operations like biofuel to agrarian biotechnology with modified fruits and veggies. The genetically modified products perform/produce better than the regular medicament. Recombinant husbandry is suitable to be further pest-resistant or weather-resistant; recombinant drugs like insulin are suitable to better work with bodies, etc. Because of the numerous benefits that recombinant DNA holds for a variety of products, experimenters are auspicious about the future it has within biosciences and in other diligence as well. **[1]**

Biotechnology plays an important role in supporting stem cell exploration, which helps the study of growing stem cells in a laboratory or in vitro. This could help in situations where patients may be experiencing sickness or disease, where embedding stem cells could help repair their vitality and give them a new lease on life. How does this function? Because stem cells can constantly divide and transfigure into other kinds of body cells, biotechnologists can learn how to work with their sui generis characters to promote the growth of specific kinds of cells. Though the exploration is in progress, it's told that the outcomes depict expectancy for the future of this special medical outlook.

What is Cyber-Security?

Cyber = Affiliated to Computer & Technologies + Security = Protection. By the name, we can introduce Cyber Security as the operation of technologies, information, data, controls to defend systems, networks, programs & devices from any cyber-attack or cyber-crime and secure pivotal documents from getting exploited. It aims to cover against cybercriminals and their unauthorized exploitation of networks and technologies. Cyber Experts exercise this strategy for guarding sensitive data of Government and United Associations and critical systems of huge companies from digital attacks. Cyber experts not only practice how to guard the systems but also can prognosticate any upcoming exploitation of currency or attacks in cyber warfare. Since Technology is getting streamlined in recent times, cybersecurity has become well known in both organizational and in person's privacy.

Research Methodology:-

This research mainly based on the statistics of data around these recent years. After pandemic hits most of the cybercrime cases are from Healthcare industry. Vulnerability of system and personal data of patients are increasing day by day because medical industry is the top most industry where a huge of data is stored and it's expensive as well .

Here shows case studies that includes cyber attacks and it's solution to prevent data from getting exploit.

Need of cyber-security in healthcare & biotech industry

Day by day medical advancements takes place. Various healthcare associations have multitudinous types of sanitarium information systems similar as EHRs, e-prescribing, practice management support, clinical decision support systems, and computerized order entry systems, and more. Not only clinical devices there are smart technologies similar as sensor elevators, Heat ventilation and air conditioning (HVAC) systems, infusion pumps, patient monitoring devices, and further to make life easier for those who work there but increases the risk of exploitation of pivotal information. **[5].** Where all kinds of trades, credits, recipient information can be tracked , all kinds of precious information of Individualities, Example- intellectual property, monetary information, patient information, their connections and more may readily be available on the internet. When everything is available free of cost the most common cyber-attack is PHISHING. Workers may unknowingly click on a malicious link or open a malicious attachment that's transferred by the perpetrator and infect their systems with malware or can spread viruses. After this malware or viruses spread via the computer network to other computers and systems. In this way, attackers can effortlessly exploit the information and damage the system. Not only they're going to damage the system but also will sell patient's information openly and that will be available for anyone to allow them to create threats over someone's privacy. Hospital staff needs to understand the privacy and security programs of the healthcare association. **[2]**

Cyber-security concerns in Biotech & Healthcare Industry

It's easy to get into the systems of such a busy association like Hospitals. Also, not many staff is good at cyber security training and may fail to act correctly when under attack. From the news, we get to know it's 10 times easier to exploit the sanitarium's information than steal someone's credit card.

Even though there are numerous experts for security but still there are exploitation conducts in huge quantities. When it comes to research there are dangerous and life threatening exploitation conducts taking place. Manipulating digital documentation is common. However, it's just a game for the

hacker to know all the sensitive information of the patients and workers in that hospital, if some party envies that association and hires a high profiled hacker.

Some common vulnerability points for a healthcare organization are as follows:

- Organization's Networks
- Internet of things
- Record disposal
- Personal devices
- Data storage
- Remote work

Improved security would reduce the threat of data theft and bolster the public's trust in the exploration community by dwindling anxiety about the possibility for unintentional exposure of information. The hype of immense practices and stakeholders by HHS, combined with a collaborative approach to compliance with security norms, analytics similar as tone- evaluation and inspection programs, would promote progress in that area.**[1] [12]**

Crucial Role of Cyber Tech in the field of Biotech & Medicine : -

It is important to protect the information in health organization and research because the collection, storage, use of large amounts of identifiable health information, which may be sensitive and crucial for work. In case of breach of security, the health information of the individual which inappropriately can be accessed by a third party, may disclose personal information that is crucial for all authentication purposes may ultimately cause intrinsic harm to that individual. Such manipulation can lead to the individual losing their job, health insurance or housing. The individual can also experience social or psychological harm. For instance, a third party has access to passport information of any patient, they can make it public, and anyone can use it for their purpose or abduct that individual for money. **[2]**

The goals of security are to ensure that (1) only authorized individuals to get required information (2) they only see the data when they need to use it for an authorized purpose (3) Use for authenticating purposes. Traditionally, these goals have been pursued through protections intended to make data processing safe from unauthorized access, alteration, deletion, or transmission. **[8]**

The importance of security of data will continue to grow as health care industry moves towards greater implementation of electronic health record access control.

Common types of Attack Vectors

Malicious Software- Malware or malicious software denotes a group of programs which is designed to execute data from a computer system without the authorization of the user. These programs carry out various functions that include altering, damaging, observing, or deleting user data. Some common malware is worms, bots, viruses, adware, Trojans, spyware, adware, backdoors, ransomware, and rootkits.

Virus- A virus is also malware, which self-replicates without the authorization of the user and infects other computers. Viruses are malicious; they're used in deleting or corrupting pivotal data. These are harnessed wide range because the easiest technique to infect a system is done by viruses. **[13]**

Trojans- Like the mythological Trojan horse, this malicious software is designed to show up as useful, licit software to get information. The most earthshaking attack Trojans can make is that they can give hackers a "backdoor" to allow access to an infected system. With help of Trojans that are penetrated in computer systems third parties effortlessly get the critical information of the association.

Spyware-Spyware is "software that's installed on a computer without the user's knowledge which transmits information about the user's computer activities over the Internet". Spyware works covertly on a system and allows the attacker to watch the target's operation and gather particular information. Spyware can come in the form of a Trojan horse employed to carry MITM attacks. Spyware can also decelerate down computers, generally by overstepping the system. **[13]**

Ransomware-This defines malware attack which demands for ransom in exchange for the decryption of information. Ransomware can use one of the several other types of malware to hack industries. Occasionally, in addition to cracking the victim's information, the hackers hang to vend or expose the information to the public if the ransom isn't paid.

Phishing- The use of social engineering (For E.g. transferring fraud links to the user) to trick individualities or associations into either discovering information or perform a dangerous activity on their computer is appertained to phishing. It's one of the most common ways to deliver malware & collect information. Attackers generally make use of emails that deflect the receiver to a website, which either collects their information or prompts the download of malicious software.

Worms-The spreading of worms in the systems depends on weakness in the target system or through social engineering. They spread extremely fast and infect the system information, causing major damage to the network. **[13]**

Analysis and Findings :-

CASE STUDY: Biotech Firms that underwent cyber-attack

- Tissue REGENIX is a leading international medical technology company with its headquarters based in United Kingdom. The company reported a cybersecurity breach in January 2020. The incident involved unauthorized access to its servers and systems and those of its third party IT service providers in the United States. It also reported that the manufacturing was temporarily disrupted and restricted its access to certain business operations after the breach.
- Miltenyi Biotec, a global biotechnology company with its headquarters in Germany announced a cybersecurity attack in November 2020. . The company reported a system outage caused by a malware attack. The attack caused issues with order and operational processes, including email and phone communications which were temporarily impaired. The Mount Locker Group claimed responsibility for the incident.
- University Hospital of Dusseldorf in Germany represents the best international hospital care, research and teaching. The organization reported a ransomware attack in September 2020, where hackers encrypt data and then demand payment to unlock it, had forced the hospital to turn the ambulance away. The attack compromised the digital infrastructures and knocked out the IT systems on which the hospital relies. A 78 year old patient's death was attributed to the attack.
- European Medicines Agency (Amsterdam, Netherlands) reported a cyber-attack in December 2020. The company notified that the documents related to Covid-19 vaccines were stolen and leaked and some crucial documents were also altered and released by the attackers.
- Health Service Executive, a healthcare system in the Republic of Ireland announced a cybersecurity breach in May 2021. The cyber-attack crippled the IT Systems in many hospitals and stole several documents. However, the attackers returned the systems for free but leaked sensitive information/data online. **[6]**
- In early April last year (2021), It was suspected that Chinese cyber espionage actors hacked into a US-based health center- a cancer research firm - with "EVILNUGGET" malware. APT22 - a Chinese group that focuses mainly on biomedical, pharmaceutical, and healthcare organizations in the past, and still they focus on the same type of field, so they targeted this same organization. The following month, numerous researchers at the MD Anderson Cancer Research reported the following concerns over financial theft of medical research on behalf of the Chinese government according to the report. As the demand increases for the usage of biomedical devices, they are vulnerable towards the target for destructive cyber-attacks said the report.

Year	The Place of Incident	Event	Risks	Amount of Loss	Suspect / Perpetrator	Measures Taken
2017	United States Bayer Healthcare Holdings LLC	NSA Cyber weapon - powered Wanna Cry Ransomware spread across the healthcare systems	Forbes reported A North Korean Cyber Criminal Organization hacked all the medical systems and stole the information and sell it to other parts of the world	200000 windows systems was hacked , Over a million of worth amount lost	North Korean Cybercriminals	U.S Government funded ICS - CERT alongside healthcare providers, Rockwell automation had to put down WannaCry advisors to assist customers.
2018	Navi Mumbai Hospital, India	Ransomeware Attack	All the informations of patient and their sensative information gone.	80 Lakh	Perpetrator is still unknown.	The case was registered under the Information Technology Act 2000. Investigation is still going on.

2019 , 22nd August	Leading India-based Healthcare Website system	Hack the system	Steal the information of Patients and Doctors	68 Lakhs	China - based Cyber Criminals	Some chinese based apps were banned and websites also

[3]

What will be the Solution?

For the sake of health research, privacy plays a crucial role to secure the personal information of patients and researchers with security measures, transparency, and accountability. These practices of security, transparency, and accountability aces in the health research setting: users should state how and why personal information is being collected, used, and secured and ensure all the information should be legally authenticated. In this way, privacy protection will help to ensure research and public trust in the medical industry.

For instance, institutions could:

- Appoint a security expert for assessing data protection and trainers for staff training.
- Make greater use of encryption and other techniques for data security.
- Implement a breach notification requirement, so that patients can have the responsibility to protect their identity in the event of a breach.
- Implement layers of security protection to prevent single points of vulnerability to security breaches.**[4]**

Effective health privacy protections require effective data security measures. The HIPAA Rule states a floor for data security standards within covered entities. Also, the survey data shows HIPAA Security Rule has improved public confidence that personal health information will be kept confidential. Therefore, all industries conducting health research should undertake measures to strengthen data protection. For instance, devices that contain patient's personal and health-related information encryption should be required for all laptops and removable media containing such data. In general, given statements among the missions and activities of institutions in the health research community, some flexibility in the implementation of specific security measures will be implemented. **[7]**

SUMMARY & CONCLUSION

The case of cyber-biosecurity isn't well-established or comprehended, even among biotechnology and cybersecurity specialists. A combined effort to evolve this arising field, define, and foster mindfulness of the dangers and formulate a common language is thus a pressing need as the digital age of biology progresses. Openings are demanded to bring together communities concentrating on these issues, and begin work on areas of common interest and the means to address the ascertain threats. Strengthened multi-stakeholder capacity is required to work at the interface between cybersecurity and biosecurity, and resources should be invested in farther understanding cybersecurity threats in the biotechnology sector in order to develop applicable counter measures.

REFERRENCES: -

1. 1.Covid outbreak in 2019 - https://www.indiatoday.in/india/story/health-sector-top-targets-cyberattacks-india-covid-pandemic-1980601-2022-07-27
2. 2.https://www.biotech-careers.org/articles/what-cyberbiosecurity#:~:text=Cyberbiosecurity%20is%20a%20field%20that,ripple%20through%20 Eastern%20gas%20stations.
3. 3.https://www.biotech-careers.org/articles/what-cyberbiosecurity#:~:text=Cyberbiosecurity%20is%20a%20field%20that,ripple%20through%20 Eastern%20gas%20stations.

1. Research gate :- A. K., & Elmedany, W. (2017, May). The effects of cyber-security on healthcare industry. In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE) (pp. 1-9). IEEE.
2. Alharam, Aysha K., and Wael Elmedany. "The effects of cyber-security on healthcare industry." In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), pp. 1-9. IEEE, 2017.
3. https://lawstreet.co/know-the-law/revenue-lost-due-to-cyber-crime-in-india - Revenue lost due to cyber-crime in India By Rashbana thansi ; Jun 04, 2021 .
4. J. J. M. Seddon and W. L. Currie, "Cloud computing and trans-border health data: unpacking US and EU healthcare regulation and compliance," Health Policy and Technology, vol. 2, no. 4, pp. 229–241.
5. https://www.hindawi.com/journals/wcmc/2019/1927495/

6. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=2a547be3425c
7. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6989022/
8. https://www.hcinnovationgroup.com/cybersecurity/article/13028304/top-ten-tech-trends-2017-medical-devices-are-the-new-cyber-threat-landscape
9. Cybersecurity Market Global Analysis- https://www.einnews.com/pr_news/621815987/v2x-cybersecurity-market-global-analysis-and-forecasts-by-solutions-component-and-application-to-2031
10. Tackling Cybersecurity Threats in the Biotechnology Industry- https://www.technologynetworks.com/informatics/blog/tackling-cybersecurity-threats-in-the-biotechnology-indu
11. Types of Cyber Attacks You Should Be Aware- https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
12. Threats in Bio - cybersecurity sec- https://www.biotech-careers.org/articles/what-cyberbiosecurity#:~:text=Cyberbiosecurity%20is%20a%20field%20that,ripple%20through%20Eastern%20gas%20stations.
13. Bio cybersecurity - https://www.ecuron.com/cybersecurity-in-biotechnology/