A COMPREHENSIVE ANALYSIS OF KEY FACTORS CAUSING VARIOUS KINDS OF CYBER-ATTACKS IN HIGHER EDUCATIONAL INSTITUTE'S

Bhoopendra Singh[1], Brijesh Kumar[2*]
[1]Ph.D Research Scholar
[2] *Prof.Dr.Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA

***Corresponding author: -** Brijesh Kumar
*Prof.Dr.Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, INDIA

Abstract- Presently, most of the educational Institute in country conducts a large numbers of academic activities in online mode for the students, researchers and other stake holders. Due to widely use of online resources, a large number of cyber attacks have been drastically increased which include the attacks on IT infrastructure, IT resources, and digital resources of online portals of reputed academic institutions and Government agencies. Cyber criminals and cyber attackers are making these attacks with the objective of destroying valuable resources and making money from this organization. Since, technological innovations are broadly used in the form of latest technology in both mode like negative and positive. Cyber attackers are using the negative mode of this technological advancement because of that it is too hard to safeguard these electronic information against cyber attacks. There are numerous forms of security algorithms available for encrypting and decrypting the classified information. Despite this, cyber criminals are finding the ways to steal the valuable information and carry out the continuous efforts by using different kinds of cyber attacks. Cyber-attackers are making the uses of virus and worms for encrypting the data and demanding a highly ransom in the form of money. In order to cater these issues, different types of security algorithms and security devices are used to identify such attacks and in case if it happens the same can be mitigate by implementing the required security solutions.

Keywords: cyber security, digital information, cyber attacks, threats and security devices.

1.Introduction

E-learning, also known as online learning or digital education has experienced substantial growth and transformation in recent years. E-learning portals, which are online platforms offering a variety of educational resources and courses, have gained immense popularity due to technological advancements, changing learning preferences, and the demand for flexible and accessible education. These platforms have democratized education, making quality learning resources accessible to

individuals who may not have access to traditional educational institutions. By breaking down geographical barriers, e-learning portals enable learners worldwide to access educational content and participate in courses remotely. This flexibility is particularly beneficial for professionals, students with other commitments, and individuals in remote areas. Moreover, e-learning supports continuous professional development and lifelong learning, allowing individuals to acquire new skills and knowledge at any stage of their lives. Despite these advantages, the increasing popularity of e-learning portals has attracted cybercriminals aiming to exploit vulnerabilities within these platforms, posing significant cyber security challenges that must be addressed.

2. Key factors of cyber security in Higher Education:-

Budget Constraints:.

Budgetary constraints serve as a formidable barrier in fortifying cyber security measures within educational institutions. The limited financial resources pose challenges in acquiring cutting-edge security tools and technologies essential for combating evolving cyber threats. Insufficient funding often hampers the implementation of comprehensive training programs, hindering the development of a vigilant workforce capable of recognizing and thwarting potential attacks. Furthermore, the scarcity of resources limits the ability to hire skilled cyber security professionals and invest in robust infrastructure, leaving systems more vulnerable to breaches and disruptions. Striking a balance between effective protection and budgetary limitations remains a constant struggle, necessitating strategic resource allocation and creative solutions to uphold adequate cyber security standards.

Diverse IT Environments: Since the use of online portals are increasing on daily basis due to the diversified IT environments and the requirement of educational institutes. During the pandemic, online mode of education was only the media which kept bonding maintain to achieve the educational goals of students as well as teachers and other stake holders. cyber security remains one of the major challenge for extending the smooth operations of these portals. Variety of IT Gazzates and other soft devices are being used by the stakeholders to carry out the academic tasks but the applications and software used by these devices were more prone to provide the access to the cyber attackers. These types of vulnerabilities are falls in the category of poor security areas hence it demands versatile security protocols. This diversity amplifies vulnerabilities, as each platform poses unique risks, vulnerabilities, and compatibility issues. Ensuring seamless integration of security measures across this heterogeneous ecosystem becomes a daunting task, often requiring intricate solutions tailored to diverse technologies. Ensuring seamless protection across different technologies while considering the diverse technical competencies of users requires a holistic

strategy. Balancing the need for stringent security measures with the flexibility to accommodate diverse systems and user preferences becomes pivotal in constructing an effective cyber security framework. Ultimately, safeguarding against threats in this diverse IT ecosystem demands an agile and inclusive approach that harmonizes security measures across the intricate web of technologies prevalent in educational environments. Various devices and platforms used by students and staff are also the key factor in increasing the complexity of cyber security.

Cultural Challenges: Academic Institute, uses highly secure and robust IT security frameworks are also posing to variety of vulnerabilities and cultural challenges. The requirement of Academic environment is quite open, research oriented and free from any kind of academic differences. It requires a complete balance of academic activities among the students and other academician. Inception of new technology and ongoing cyber attacks have been creating a new way for protection of data and information by implementing various data protection policies and frameworks. It is utmost need of todays world to create the balance between academic freedom and data protection. Due to the change of cultural in academic domain and also due to paradigm shift from classroom teaching to hybrid mode or blended mode of teaching, the security of online databases and research repositories have become one of the prime factor to deal with it. IT Security risks with infrastructure and various applications are leading to disasters and loss of valuable information with a demand of huge financial losses. Security vertical of such applications and portals are making more harden by implementing security policies, security protocols and deploying the latest IT security tools and devices.It has become a shared responsibility of academic users and security person to safeguarding the sensitive information. Finally, discussing the various IT security issues due to the change of cultural shift has to be taken care on priority to preserve and increase the widely use of academic resources academic institutions.

Resource Limitations: Due to the limitation of various IT resources and security policies, academic institutions are bound to face lots of obstacles in academic freedom. Due to high cost of security devices and IT infrastructure required to implement the same are totally un balanced and leading to security breaches in the form of various cyber attacks and data breaches. Cost of IT trained manpower and required skill set have also become a major challenge to deal with it due to which lots of organisationa are facing security compromising issue bearing a lots of data losses.Most of the web applications are requiring continuous update for which a experienced and skilled professional are required. Hence, budget allocation to higher academic institute is a major challenge to cater with ongoing cyber threats and cyber attacks on IT portals and aplications. Due to the inception of new era of technology, cyber audit has also become one of the prime need to know

any security issues in IT resources which include entire IT resources like infrastructure, resources and security devises.

3.Review of the Literature

Singh and Kumar (2020) delve into the critical importance of cybersecurity in the domain of higher educational Institute. Their study highlights the various threats and vulnerabilities that online education platforms face and suggests comprehensive security measures to mitigate these risks. They emphasize the need for robust authentication mechanisms, secure communication channels, and regular security audits to safeguard educational data and ensure the integrity of e-learning resources and systems. Scott and Vanoirbeek (2020) explore the advancements in technology-enhanced learning (TEL) and its implications for modern education. They provide an in-depth analysis of how technological innovations, such as artificial intelligence and adaptive learning systems, are revolutionizing educational practices. The paper also discusses the challenges associated with implementing TEL, including the necessity for robust cyber security measures to protect sensitive information in digital learning environments. The Information Commissioner's Office (ICO) (1998) presents an overview of the Data Protection Act 1998 and its relevance to the BYOD trend in educational settings. The document underscores the legal obligations institutions must adhere to when handling personal data and the specific cybersecurity concerns that arise when students and staff use their own devices for academic purposes. It advocates for stringent data protection policies and regular security training to mitigate potential risks. Moneo, Caballe, and Prieot (2012) address the security challenges inherent in learning management systems (LMS). Their research identifies common vulnerabilities in LMS platforms and proposes a multi-layered security approach to counteract these threats. The authors stress the importance of incorporating encryption, user authentication, and regular security updates to protect the integrity and confidentiality of educational content and user data. Johnson (2007) examines the role of asynchronous discussion boards in facilitating knowledge construction in e-learning environments. Through a qualitative analysis of student perceptions, the study reveals the significant impact of secure and well-moderated online discussions on the learning experience. The paper highlights the need for secure communication channels to ensure student privacy and data protection in e-learning platforms. Report by Universities UK (2013) outlines the various cyber security risks faced by higher education institutions and offers strategic recommendations for managing these threats. It emphasizes the importance of developing a comprehensive cybersecurity framework that includes risk assessment, incident response, and continuous monitoring. The document also calls for

increased collaboration between universities and cyber security experts to enhance the overall security posture of educational institutions. Nickolova and Nickolov (2007) propose a detailed threat model for user security in e-learning systems. Their research identifies potential threats to user data and system integrity, including phishing attacks, unauthorized access, and data breaches. The authors recommend a proactive approach to security, involving regular threat assessments, user education, and the implementation of advanced security technologies to protect e-learning environments. Rjaibi et al. (2012) present a comprehensive framework for measuring cybersecurity in e-learning systems. Their study emphasizes the need for a multi-dimensional approach to security assessment, covering technical, organizational, and human factors. The authors provide practical guidelines for implementing effective cybersecurity measures and stress the importance of continuous monitoring and evaluation to maintain a secure e-learning environment. Weippl (2005) explores the various security issues related to e-learning platforms and offers insights into best practices for ensuring a secure online learning experience. The article discusses the importance of data encryption, secure user authentication, and regular system updates in preventing security breaches. Weippl also highlights the role of user awareness and training in maintaining a secure e-learning environment. Anwar and Greer (2011) investigate the use of role- and relationship-based identity management systems to enhance privacy in e-learning environments. Their research demonstrates how such systems can provide granular access control and protect user identities while facilitating collaboration and information sharing. The authors advocate for the integration of advanced identity management solutions in e-learning platforms to ensure privacy and security. Wolpers and Grohmann (2005) examine the application of technology-enhanced learning in the corporate sector, emphasizing the importance of secure knowledge distribution. Their study highlights the need for robust cybersecurity measures to protect sensitive corporate information and ensure compliance with regulatory requirements. The authors suggest adopting comprehensive security policies and advanced technological solutions to safeguard corporate e-learning initiatives.

4. Cyber Space Threats

Preserving the IT systems and IT infrastructure having sensitive data and information are the main areas of cyber threats to be targeted by the cyber criminals. Cyber threats are the part of vulnerable activities which are performed by the cyber criminals, hackers and even by the person of an organization internal security team. Cyber threats aiming to malicious acts including virus attacks, worms attacks, phishing attacks, SQL injection and DDOS attacks. Ransomware is also one of the dangerous attacks which destroy entire information and data stored in local devices, servers and over network. It demands a huge amount of money to get the data back once this attack has happened. It has become a major cyber challenge to Academic Institute, Government and other

various business organizations due to its citizen centric database and infrastructure. Recently attacks held on Microsoft has impacted a lot on Airline, Banking, Railways and other various operations which brought these operation on hault and caused lots of monitoring and trouble to the citizen of world. Since all the citizens are dependent on the IT resources and it has become a part of day to life of n individual there is a prime need of everyone to secure this from emerging various kinds of cyber attacks.

Normally, it is the extent of the worldwide internet, which makes endlessly covering areas for public entertainers with various legitimate and social methodologies and different vital interests. Accordingly, the security undertakings and elements of every nation are progressively impacted by the internet. Clients can change or control the product and equipment they use. Its a well known fact that few individuals can really on control or oversee digital fighting.

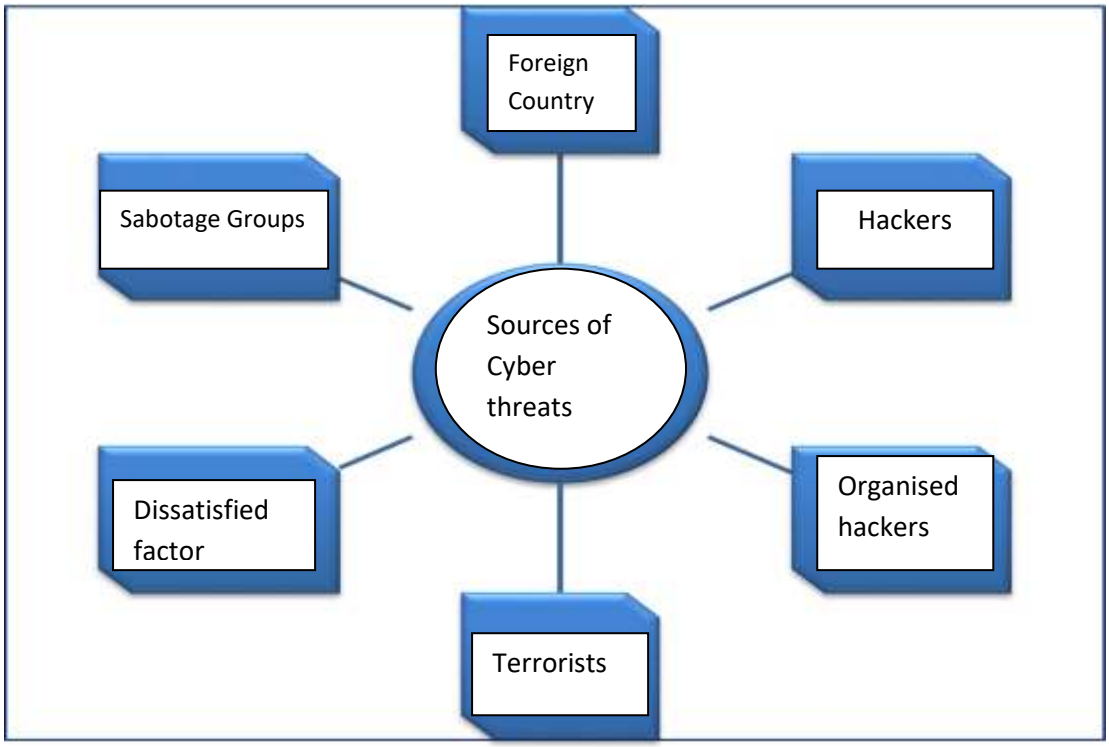

Fig. 3. Sources of cyber threats

The essential dangers in the internet are: unfamiliar dangers, interior dangers, and dangers in the store network of labor and products, and dangers because of deficient functional capacity of neighborhood powers. One more wellspring of assaults is gatherings who assault digital frameworks to bring in cash, and the assaults of these gatherings are. In the ongoing circumstance, it is feasible to penetrate networks with at least information and abilities, by downloading the fundamental projects and conventions from the Web and utilizing them against different locales.

Cyber attacks and threats are the parts an array which constitute variety of cyber risks and harmfull assets for stealing and destroying the critical information and infrastructure. Higher educational and

research institute maintains a rich and research oriented data for carrying out the research and development activities of various domains. It requires a lots of effort and huge investment of money and expenditure on laboratory equipments. Security of such equipment and devices from cyber threats has to be ascertain by the users and owners of such resources. Malware attacks on equipments and highly used application will not only infect the resources but also destroy entire research and academic activities.

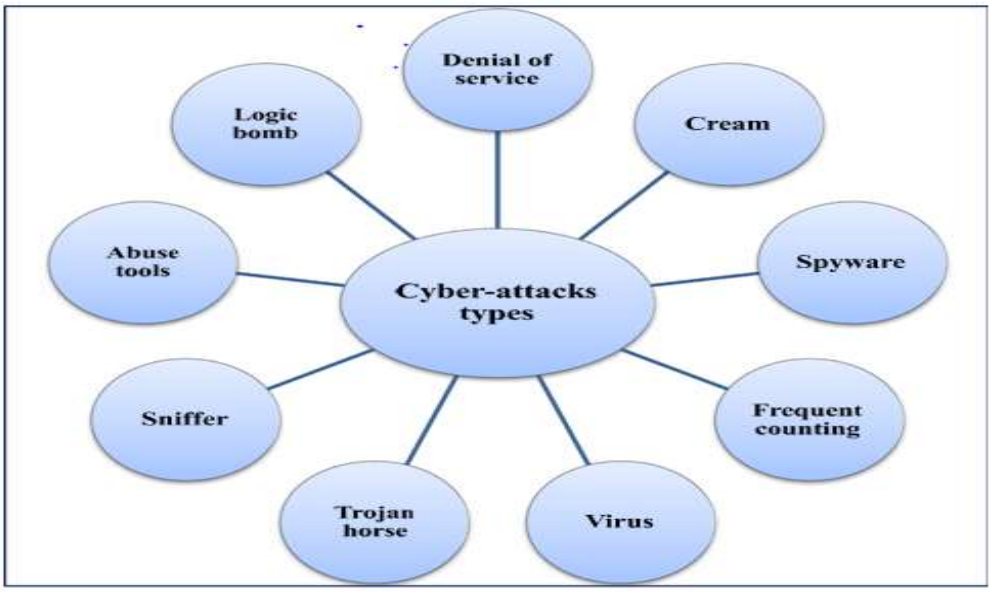

Fig. 4. Major types of cyber attacks

Moreover, an infection befouls framework documents, which are usually practicable projects, by embedding a duplicate of it into those records. By stacking contaminated documents into memory, these adaptations run and permit the infection to taint different records. In contrast to worms, infections require human mediation to spread. Then again, the worm is an independent framework program that recovers itself by duplicating starting with one PC then onto the next in the organization. At last, Botnet is an organization of contaminated controller frameworks, which is utilized to disperse malware, coordinate assaults, and spam and take messages. Botnets are typically furtively introduced on the objective PC, permitting the unapproved client to remotely control the objective framework to accomplish their pernicious objectives.

5. Cyber-security

For calculating cyber threats, we need to formalize the process of risk assessment in cyber security. This involves understanding the components of cyber threats, quantifying their likelihood and impact, and combining these factors to compute the overall risk. Below is a theorem along with its mathematical formulation and explanation.

Cyber Threat Risk Theorem

Given a set of cyber threats {T1,T2,…,Tn} the risk Ri is associated with each threat Ti can be calculated as:

Ri=Pi×Ii

where:

- Pi is the probability of occurrence of threat Ti
- Ii is the impact of threat Ti if it occurs

The overall risk R_{total} to the system is the sum of the risks of all individual threats:

$$R_{\text{total}} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} (P_i \times I_i)$$

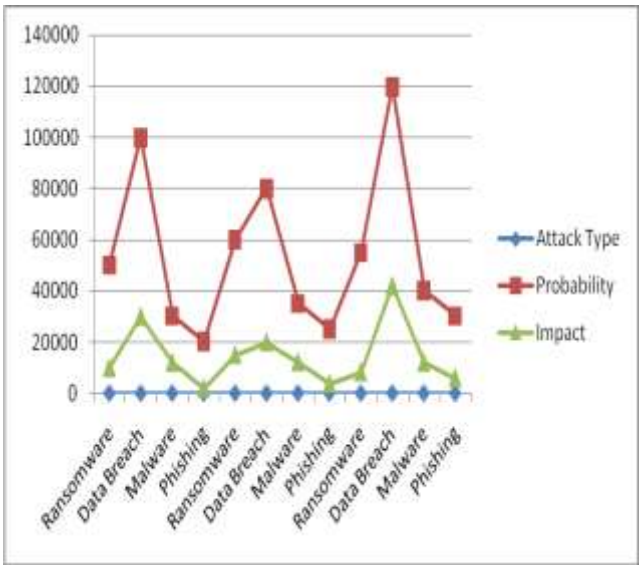

Fig:- 5 various attacks with probability and impact

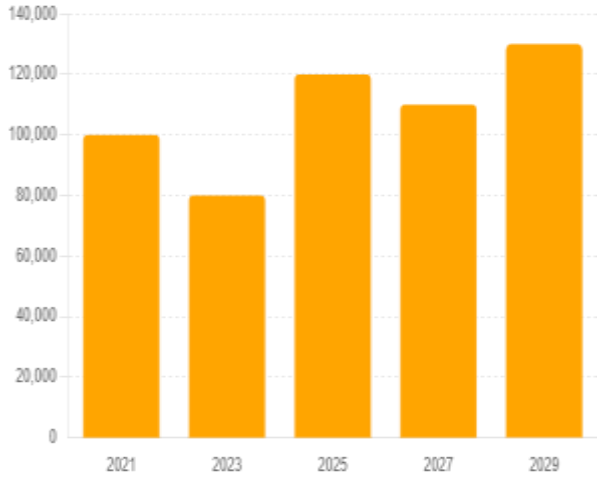

Fig:- 6 Total (Actual/ Expected) Impact of Data Breaches by Year

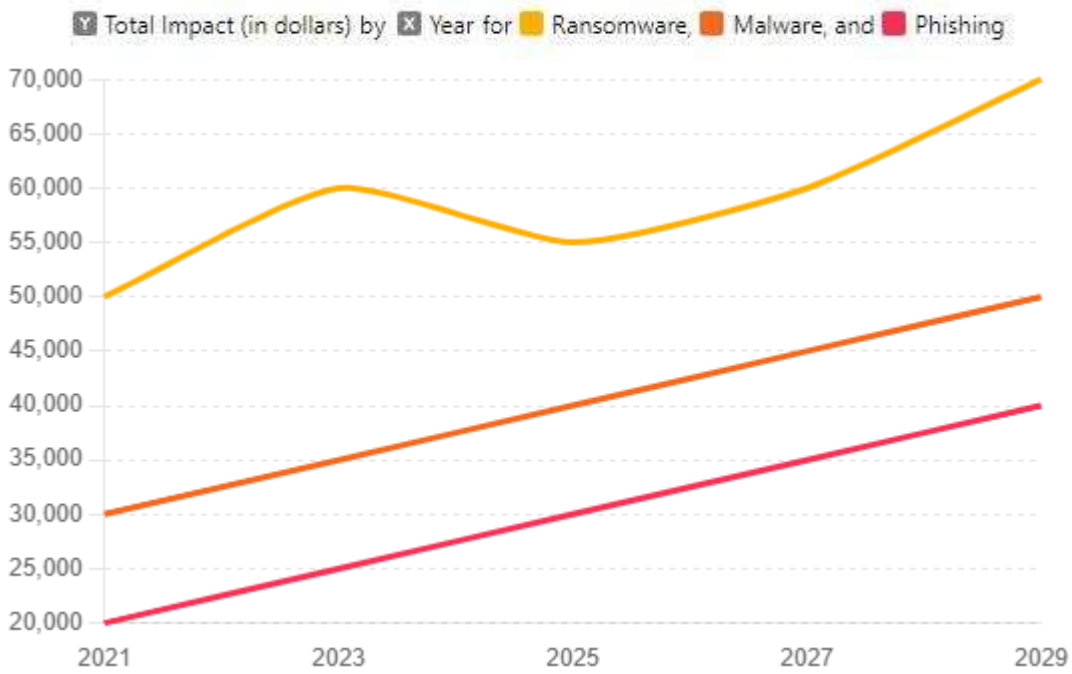

Fig:-7 Total Impact of Different Attack Types by Year

The overall analysis of various types of cyber attack data with calculated cyber risks provides crucial results based on the ongoing trends and impacts of cyber attacks .Comparative analysis of these attacks as mentioned in table like ransom ware, malware, phishing, and data breaches, help us to calculate the probability of risks over the years. Projected charts and graphs depicts about the risks helping expected losses and mitigation mechanism required to prevent the highest potential for damage, guiding organizations in prioritizing their cyber security efforts and resource allocation. Furthermore, the identification of incoming network traffic using latest security devices also helps in examination of source and destination IP addresses involved in these attacks. This comprehensive trend to identify cyber attack data tells that the institutions and other organizations are to be more equipped with cyber tools to counter such threats and also to mitigate risks, respond to incidents, and enhance their overall cyber security posture.

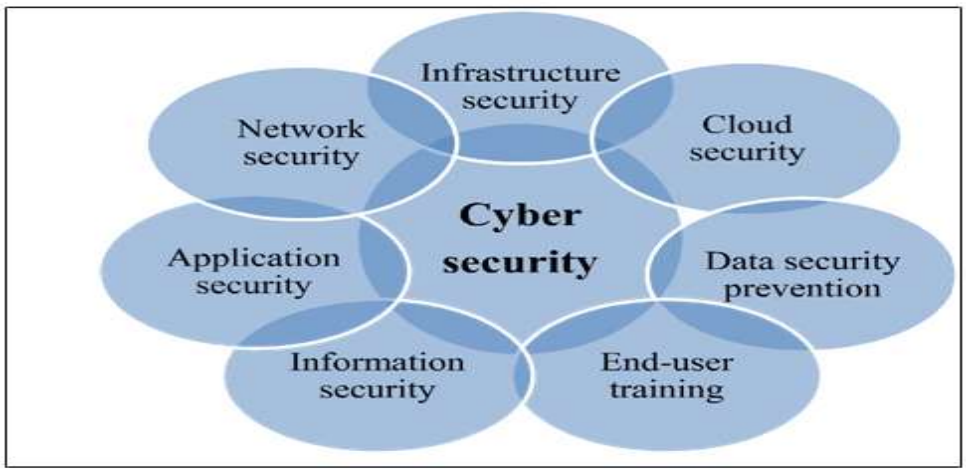

Fig. 8. various types of cyber security

More on cyber security involves the security of Network, Infrastructure, Clouds, Data Security, end user, information and application security. These are the major pillars where the impact of cyber security is to be analyses on regular basis by taking necessary steps for its improvement. These critical areas are more prone to cyber attacks due to the role and importance in the domain of cyber security. Higher Education institute and other government organizations to set a priority of their cyber security goals by putting their best efforts to identify such attacks and also to implement corrective measures.

Cyber security also focus on the CIA triad—Confidentiality, Integrity, and Availability—known as foundational concept in cyber security, providing and functioning as guiding principles for protecting information systems. “Confidentiality” defines that any kind of sensitive information is to be accessed by authorized individuals, which helps in maintaining privacy and avoiding unauthorized access. “Integrity” ensures the accuracy and reliability of data, which means that the data remains unaltered and trustworthy throughout its lifecycle. “Availability” provides the feature of information and data are accessible to authorized users only as per the need and requirement, preventing disruptions in service and maintaining operational continuity.

.

Fig. 9. Security triangle CIA

6. Conclusion

Cyber security plays a vital role in understanding the recent trends of cyber threats and its impact in the domain of higher educational institute. These kinds of attacks like ransom ware, malware, phishing, and data breaches, are damaging the image of Institution and also incurred with huge financial and academic losses. It is sole responsibility of a security expert of these organization to keep the things and devices intact by regular updated, synching with latest trends of technology and also by implementing the defined cyber policies in the organizations. In order to understand the risks, impact and expected losses out of these attacks , a robust and essential mitigation mechanism required to prevent the highest potential for damage, guiding organizations in prioritizing their cyber security efforts and resource

allocation. Various kinds of security algorithms and theorems are to used to identify the entire network traffic and in case of any finding the same are to analyse by using latest trends of artificial intelligence and machine learning techniques to read and understand the behavior and accordingly the required solution may be designed. The data stored by these higher educational Institute are too crucial from the point of research and development and strict line of defence are to maintain to keep this data safe for the use of researcher and other stake holders.

References

1. Singh, Bhoopendra, and Brijesh Kumar. "Role of Cyber Security in E-Learning Education." *International Journal of Advanced Science and Technology*, vol. 29, no. 4s, 2020, pp. 3172-3178.

2. Scott, P., and C. Vanoirbeek. "Technology-Enhanced Learning." *International Journal of Advanced Science and Technology*, vol. 29, no. 4s, 2020, pp. 3172-3178.

3. "Data Protection Act 1998; Bring Your Own Device (BYOD)." ICO, 1998, http://ico.org.uk/. Accessed 20 Sept. 2014.

4. Moneo, J. M., S. Caballe, and J. Prieot. "Security in Learning Management Systems." *eLearning Papers*, Catalonia, Spain, 2012.

5. Johnson, H. "Dialogue and the Construction of Knowledge in E-Learning: Exploring Students' Perceptions of Their Learning While Using Blackboard's Asynchronous Discussion Board." *European Journal of Open, Distance and E-Learning*, 2007.

6. "Cyber Security and Universities: Managing the Risk." Universities UK, Nov. 2013, http://www.universitiesuk.ac.uk/. Accessed 25 Sept. 2014.

7. Nickolova, M., and E. Nickolov. "Threat Model for User Security in E-Learning Systems." *International Journal "Information Technologies and Knowledge"*, vol. 1, 2007, p. 341.

8. Rjaibi, N., L. B. A. Rabai, A. B. Aissa, and M. Louadi. "Cyber Security Measurement in Depth for E-Learning Systems." *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 11, 2012, pp. 1-15.

9. Weippl, E. R. "Security in E-Learning." *eLearn Magazine*, 2005, http://elearnmag.acm.org/. Accessed 25 Sept. 2014.

10. Anwar, M., and J. Greer. "Role- and Relationship-Based Identity Management for Privacy-Enhanced E-Learning." The University of Saskatchewan, Department of Computer Science, 2011.

11. Wolpers, M., and G. Grohmann. "Technology Enhanced Learning and Knowledge Distribution for the Corporate World." *International Journal of Knowledge, Learning*, 2005.

12. Sood, S. K. "Phishing Attacks: A Challenge Ahead." *eLearning Papers*, Apr. 2012, http://www.openeducationeuropa.eu/en/paper/cyber-security-and-education. Accessed 25 Sept. 2014.

13. May, M., and S. George. "Privacy Concerns in E-Learning: Is Using a Tracking System a Threat?" *International Journal of Information and Education Technology*, vol. 1, no. 1, Apr. 2011, http://liris.cnrs.fr/Documents/Liris-5266.pdf. Accessed 25 Sept. 2014.

14. Alw, N., and I.-S. Fan. "E-Learning and Information Security Management." *International Journal of Digital Society*, vol. 1, no. 2, June 2010.

15. Graf, F. "Providing Security for E-Learning." *Computers & Graphics*, vol. 26, no. 2, 2002, pp. 355-365.

16. Chen, Y., and W. He. "Security Risks and Protection in Online Learning: A Survey." *The International Review of Research in Open and Distance Learning*, 2013, http://www.irrodl.org/index.php/irrodl/article/view/1632/2712. Accessed 15 Sept. 2014.

17. Rabai, L. B. A., and N. Rjaibi. "Quantifying Security Threats for E-Learning Systems." *Education and e-Learning Innovations (ICEELI), 2012 International Conference*, Tunis, Tunisia, July 2012.

18. Nandy, Debarshi. *Securing E-Learning Systems*.

19. Aggarwal, Anil. *Security for E-Learning*.

20. Hengge, Monika, and Christian Winkler. *E-Learning Security*.

21. Clark, Ruth C., and Richard E. Mayer. *E-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning*.

22. Elkins, Diane, and Desiree Pinder. *E-Learning Uncovered: Articulate Storyline 360: 2nd Edition*.

Online Resources:

23. "EDUCAUSE Review: Offers Articles and Resources Related to E-Learning Security." *EDUCAUSE Review*, www.educause.edu/review. Accessed 18 July 2024.

24. "NIST (National Institute of Standards and Technology) Guidelines and Publications: Includes Guidelines on Securing E-Learning Systems." *NIST Cybersecurity Publications*, www.nist.gov/cyberframework/online-learning/informative-references. Accessed 18 July 2024.

25. "OWASP (Open Web Application Security Project): Provides Guidance on Securing Web Applications, Which Are Often a Component of E-Learning Portals." *OWASP Website*, www.owasp.org. Accessed 18 July 2024.