Journal of Research Administration
Society of Research Administrators International

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- Currently, the majority of the activities conducted by the educational institution and the interactions that are associated with it at all levels—involving persons, researchers, and other stakeholders—take place online mode. Cybercriminals have recently been targeting IT infrastructure, IT resources, and online application portals in a number of reputable educational institutions and government agencies across the globe.This has become a challenging issue for safeguarding the electronic information against cyber attacks. Cyber-attacks are intended to do harm to these educational institutions by stealing research data and other pertinent information, as well as causing damage to their IT infrastructures. Some of the harms are: Data distribution services (DDS), computer infections, knowledge gaps, and other attack vectors. Different associations utilize different answers for forestall harm brought about by digital assaults. Network safety follows constant data on the most recent IT information. In order to cater these issues, different strategies had been proposed by specialists all over the planet to forestall digital assaults or decrease the harm brought about by them. A portion of the strategies are in the functional stage and others are in the review stage. The point of this study is to overview and extensively survey the standard advances introduced in the field of digital protection and to explore the research possibility to find out the difficulties, shortcomings and qualities of the proposed strategies. Various sorts of new digital assaults are being investigated exhaustively across the globe. Standard security systems are examined, alongside the historical backdrop of network protection and early age techniques. Also, arising patterns and late advancements in digital protection, as well as security dangers and difficulties, are presented. It is stated that the extensive survey related to IT and digital protection will be helpful in digging out the issues and challenges related to cyber attacks and also to resolve these.

Keywords: IT security, Electronic information, cyber attacks, threats and emerging trends.

Introduction

In the present era, the utilization of the Web has expanded exponentially and established its availability in terms of existence essentially to every individual everywhere. Developments in this field and low expenses have drastically expanded the accessibility, use and execution of the internet, due to that it is estimated that today the Web has around 4 billion clients around the world (Tan et al., 2021). The Web has made a gigantic worldwide organization that has produced huge amount of money yearly for the worldwide economy (Judge et al., 2021). Right now, most monetary, business, social, social and regulatory exercises and discussions at all degrees of states, including people, non-legislative associations and state and government organizations, happen in the internet (Aghajani and Ghadimi, 2018). Basic and delicate frameworks are either themselves are the part of the internet or they are controlled. most of media exercises move to this space, most of monetary trades happen through this space. The portion of the pay of the internet organizations in the GDP (Gross domestic product) of nations has expanded fundamentally, and the internet markers have an enormous piece of the pointers that action the degree of improvement. A critical piece of the material and scholarly capital of the nations is utilized for this space, and a huge piece of the material pay and scholarly accomplishments of the residents (Amir and Givargis, 2020). At the end of the day, different parts of a resident's life are in a real sense associated with this space, and unsteadiness, weakness and challenges in this space. Nonetheless, the development of the internet has introduced new security dangers to state run administrations and people, for example, digital fighting, cybercrime and digital psychological warfare, as well as digital surveillance (niraja and srinivasa rao, 2021). The distinction between digital dangers and conventional public safety dangers is that digital dangers are considerably more straightforward in nature and their entertainers are legislatures and states that can be recognized in a specific geological region, and this has made public safety in the customary sense be tested and incapable here (Sarker (2021)). There are various circumstances for serious and at times limitless physical or money related hurt, including the capacity of a contamination that pursues the money related records of a monetary structure or upsets a country's protections trade, or by sending an off-base message, it will cause the country's influence plant to respite and miss the mark, or even by upsetting the flight authority system, it will cause air disasters (Snehi and Bhandari, 2021; Ahmed Ja-mal et al., 2021). Along these lines, until lawmaking bodies prepare a sensible importance of a computerized attack that is recognized and leaned toward by the worldwide neighborhood, will decidedly be really provoking for experts to address the confounded and various viewpoints and portions of the issue and give legitimate urging and assessment. Consequently, the request that arises is a computerized attack, what are its characteristics and whether any attack that occurs in the web can be seen as a kind of attack in its customary and model sense or not (Gupta Bhol et al., 2021). The presence of a broad importance of a computerized attack will beyond a shadow of a doubt clearly influence the legitimate environment to continue and recognize the results of this attack type (Furnell et al., 2020). There is no doubt that the shortfall of an obvious and expansive definition mists the really legal way. As such, the importance and need of having an alright definition, fundamentally for the beginning of the subject and its explanation, change and assessment is crucial, and a point by point study is significant. Finally the completion of the paper is presented.

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

Budget Constraints: Budgetary constraints significantly impede the implementation of robust cybersecurity measures within institutions. Insufficient funding limits the acquisition of advanced security technologies and impedes the adoption of updated systems, leaving networks and data vulnerable to evolving threats. Moreover, budget limitations often curtail comprehensive staff training and education programs, hindering the development of a vigilant and proactive cybersecurity culture. Understaffing or a lack of expertise due to constrained budgets further amplifies vulnerabilities, impacting incident response and recovery capabilities. Consequently, these constraints force difficult prioritization decisions, potentially leaving critical aspects of cybersecurity unaddressed. Despite the crucial need for comprehensive protection, financial limitations continue to challenge the establishment of resilient cybersecurity frameworks within higher educational institutions.

Budgetary constraints serve as a formidable barrier in fortifying cybersecurity 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 cybersecurity 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 cybersecurity standards.

Diverse IT Environments: The diverse IT environments within the realm of cybersecurity present multifaceted challenges for safeguarding educational institutions. The expansive array of devices, operating systems, and applications utilized by students, faculty, and staff creates a complex landscape that 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. Moreover, the varying levels of technical proficiency among users further complicate security efforts, necessitating comprehensive strategies that accommodate this wide-ranging spectrum of devices and user competencies. Addressing cybersecurity in such a diverse IT environment demands adaptive and inclusive approaches that account for the intricate interplay of technologies and user behaviors while ensuring cohesive protection across the entire technological spectrum. Cybersecurity faces a formidable challenge within diverse IT environments prevalent in educational institutions. The proliferation of devices, operating systems, and applications across campuses creates a labyrinth of vulnerabilities. Each platform introduces its unique set of security risks and compatibility issues, necessitating a versatile approach to defense. Managing security across this varied landscape demands constant vigilance and adaptability. 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 cybersecurity 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: Cultural challenges pose a significant hurdle in establishing robust cybersecurity frameworks within educational institutions. The academic culture often values openness, collaboration, and the free flow of information, which can inadvertently conflict with stringent security protocols. Balancing the principles of academic freedom and knowledge sharing with the imperative need for data protection becomes a delicate tightrope walk. Cultivating a cybersecurity-conscious culture amidst this ethos requires a paradigm shift, emphasizing the shared responsibility of safeguarding sensitive data. Encouraging a mindset that prioritizes security without stifling collaboration demands a comprehensive approach involving education, policy development, and ongoing dialogue. Achieving this balance necessitates not only technological solutions but also a cultural transformation that instills a deep-seated awareness of cybersecurity risks and responsibilities among all stakeholders, fostering a harmonious synergy between academic values and robust security measures.

Cultural challenges in cybersecurity present a unique landscape within educational institutions. The academic environment, inherently open and collaborative, often clashes with the need for stringent cybersecurity measures. Encouraging a culture that values information sharing and collaboration while emphasizing the importance of data security requires a delicate balance. Bridging this gap involves fostering awareness and understanding among faculty, students, and staff about the criticality of cybersecurity without stifling the academic ethos. It necessitates creating policies and practices that integrate security seamlessly into daily operations, promoting a mindset where cybersecurity is seen not as an impediment but as an essential part of academic integrity. Ultimately, addressing cultural challenges in cybersecurity involves a cultural shift, embedding a proactive approach to security within the fabric of the institution's values and practices while preserving the collaborative spirit fundamental to academia.

Resource Limitations: Resource limitations present a formidable obstacle in the pursuit of robust cybersecurity within educational institutions. The shortage of skilled cybersecurity professionals and inadequate financial allocations significantly impact the implementation of effective security measures. With a limited pool of experts and constrained budgets, institutions face challenges in acquiring cutting-edge technologies, conducting comprehensive security audits, and maintaining updated systems. These constraints not only hamper proactive threat identification and mitigation but also impede the establishment of strong incident response protocols. Consequently, educational institutions often find themselves navigating a landscape where the demand for comprehensive cybersecurity surpasses available resources. Addressing resource limitations in cybersecurity

requires creative solutions, including partnerships with external agencies, leveraging open-source tools, and fostering a culture of shared responsibility among staff and students. Overcoming these constraints necessitates strategic allocation of resources and advocating for increased funding to fortify the cybersecurity posture of educational institutions.

Underneath referenced, five situations can be considered for digital fighting:

(1) Government-supported digital undercover work to assemble data to design future digital assaults,

(2) a digital assault pointed toward laying the preparation for any distress and well known uprising,

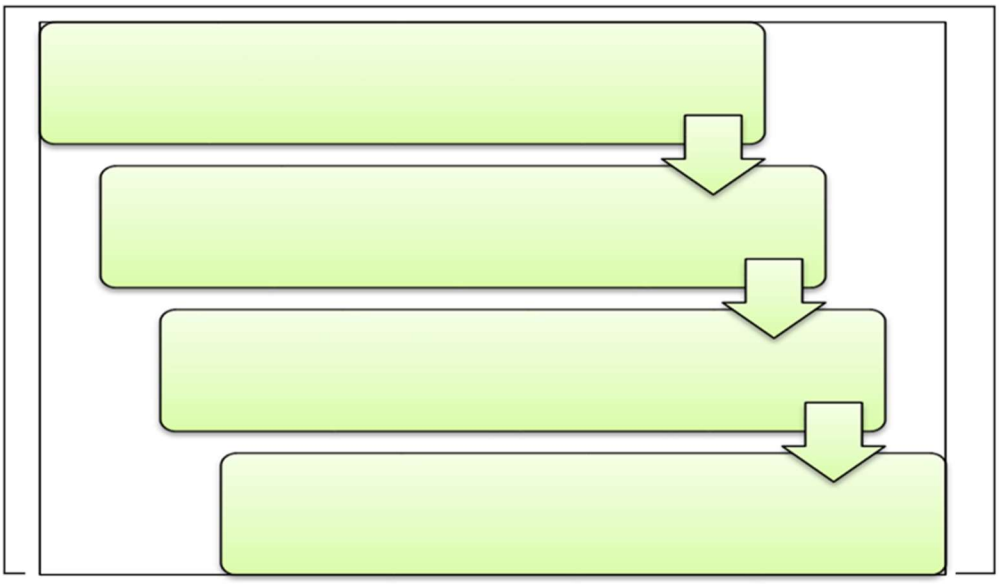
(3) Digital assault pointed toward handicapping gear and working with actual hostility,

(4) Digital assault as a supplement to actual hostility, and

(5) Digital assault with the point of far and wide obliteration or disruption as a definitive objective (digital fighting) (Alibasic et al., 2016).

2.1. Meaning of digital assault according to the experts' perspective:-

In the realm of cybersecurity, a digital assault, often referred to as a cyber-attack, signifies a deliberate, malicious attempt to compromise, disrupt, or gain unauthorized access to digital systems, networks, or data. From the perspective of cybersecurity experts, a digital assault encompasses a wide array of tactics and techniques employed by threat actors to exploit vulnerabilities, steal sensitive information, disrupt operations, or cause damage to digital assets. These assaults can take various forms, including phishing attacks, ransomware, malware infections, DDoS (Distributed Denial of Service) attacks, and insider threats, among others. The essence of a digital assault lies in its intent to infiltrate, manipulate, or harm digital infrastructure, making it a critical concern for cybersecurity professionals tasked with safeguarding systems and data against such threats .In the examination and scrutinize of this definition, one might say that the three components, like specific the culprit of the assault, the reason and goal of the assault, have been utilized as models.



From the perspective of cybersecurity experts, a digital assault refers to a deliberate and targeted attack on digital systems, networks, or assets with the intent to compromise, disrupt, or gain unauthorized access. These attacks are orchestrated by threat actors who exploit vulnerabilities in software, hardware, or human behavior to breach security defenses. Digital assaults encompass a wide range of techniques, including malware infections, phishing attempts, ransomware attacks, DDoS (Distributed Denial of Service) attacks, and social engineering tactics. The primary goal of these assaults is often to steal sensitive information, disrupt services, extort money, or cause damage to digital infrastructure. Cybersecurity experts focus on understanding, preventing, and mitigating these attacks by employing various defense mechanisms, such as firewalls, intrusion detection systems, encryption, and incident response plans, to protect against the constantly evolving landscape of digital threats. Considering what is happening, one might say that the referenced definition is generally fragmented and does exclude a critical piece of the assaults completed by private and non-legislative gatherings (Zhang, 2017).

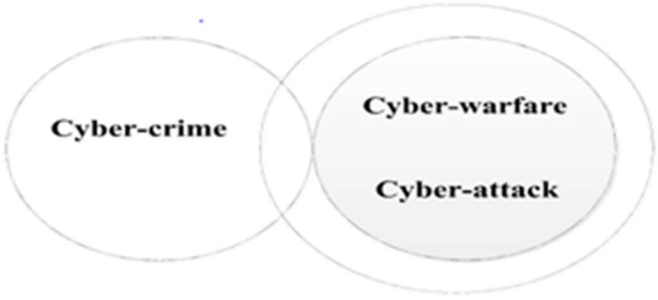


Fig. 2. Distinction between cyber-crime, cyber-warfare, and cyber-attack.

Table 2
Distinction between cyber-crime, cyber-attacks, and cyber-warfare (Zhang, 2017; Dash et al., 2021).

Type of cyber action	Nature and characteristics
Cyber-crime	Cyber actions taken only by non-governmental attackers.
Cyber-crime	The cyber action is carried out by a computer system and is merely in violation of criminal law.
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network.
Cyber-attack and cyber-warfare	The attack must have political or security purposes.
cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an armed attack.

(2) Michael Hayden: Michael Hayden, a former director of the NSA and the CIA, views digital assaults as deliberate and targeted actions aimed at compromising, disrupting, or infiltrating digital systems for various motives. Hayden often emphasizes the evolving nature of these assaults, ranging from traditional hacking methods to more sophisticated cyber warfare tactics orchestrated by nation-states or state-sponsored entities. According to Hayden, digital assaults encompass a broad spectrum of cyber threats, including cyber espionage, cyber terrorism, and cyber warfare, all with the potential to disrupt critical infrastructure, steal sensitive information, or cause significant damage. He emphasizes the need for robust cybersecurity measures, international cooperation, and a nuanced understanding of the geopolitical implications of digital assaults in today's interconnected world. Any intentional undertaking to upset or demolish another country's PC associations (Robinson et al., 2015). The broad arrangement of the standards of war leaves free the web, which can doubtlessly have unsafe and troublesome implications for the spread of war and hawkishness of countries (Edgar and Manz, 2017). Diverged from the primary definition, which limited the guilty parties of the attack to government aggressors, this definition is general that it is easy to unravel and, as referred to, can be risky and make unfavorable results and make disturbance in relations among countries and ultimately a threat to concordance at the level of the overall neighborhood (et al., 2012).

(3) Martin Libicki: Martin Libicki, a notable cyber warfare expert, perceives digital assaults as deliberate and targeted actions directed at exploiting vulnerabilities within digital systems, networks, or infrastructure. From Libicki's perspective, these assaults encompass a spectrum of cyber threats that may include cyberattacks launched by various actors, ranging from individual hackers to nation-states or state-sponsored entities. He emphasizes the strategic nature of these assaults, highlighting their potential to disrupt critical infrastructure, compromise sensitive data, or cause significant economic and societal impacts. Libicki often underscores the importance of understanding the motives behind digital assaults, the evolving tactics employed by attackers, and the necessity for robust cybersecurity strategies to mitigate these threats effectively. (Damon et al., 2014; Shamel et al., 2016)

(4) Tallinn Manual Group: The Tallinn Manual is a non-binding document compiled by a group of legal experts, discussing the application of international law to cyber conflicts. The group behind the Tallinn Manual considers digital assaults within the context of cyber operations that can potentially trigger state responsibility under international law. In this framework, a digital assault refers to a cyber operation conducted by a state against another state, constituting a use of force or an armed attack. The group identifies digital assaults as actions that cause damage, injury, or destruction to another state's infrastructure, which could provoke lawful countermeasures or responses under international law. The Tallinn Manual seeks to provide guidance on how existing international laws, such as those pertaining to armed conflicts and the laws of war, apply to cyber operations and digital assaults conducted by states. (Bullock et al., 2021). Accordingly, the fundamental premise of the meaning of this gathering is the outcome arranged nature of digital assaults, not the actual assaults; Along these lines, assuming that this sort of assault leaves the

impacts and outcomes of brutality, unbiased and substantial, it will be depicted as an assault, and it is at this stage that the standards of worldwide regulation in related regions and fields (the option to engage pressure, the law of war and the law of global obligation will be enforceable (Chen et al., 2021).

3. Cyber space threats

Cyberspace threats represent a diverse and evolving landscape of risks that target digital systems, networks, and data. These threats encompass a wide range of malicious activities orchestrated by various actors, including hackers, cybercriminals, state-sponsored entities, and even insiders. Cyber threats include but are not limited to malware attacks aiming to infiltrate systems, phishing attempts to trick users into revealing sensitive information, ransomware demanding payment for data release, DDoS attacks disrupting online services, and sophisticated cyber espionage campaigns aiming to steal valuable information. The interconnected nature of our digital world amplifies these threats, presenting challenges for individuals, businesses, governments, and critical infrastructure. Addressing cyberspace threats requires a multifaceted approach involving robust cybersecurity measures, continuous threat intelligence gathering, user education, international cooperation, and the development of resilient systems capable of withstanding evolving cyber threats

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 (Iqbal and Anwar, 2020). Accordingly, the secu-rity undertakings and elements of every nation are progressively impacted by the internet (Zhao et al., 2020).. Clients don't can change or control the product and equipment they use. Its a well known fact that few individuals can really control or oversee digital fighting (Zhang et al.2021.

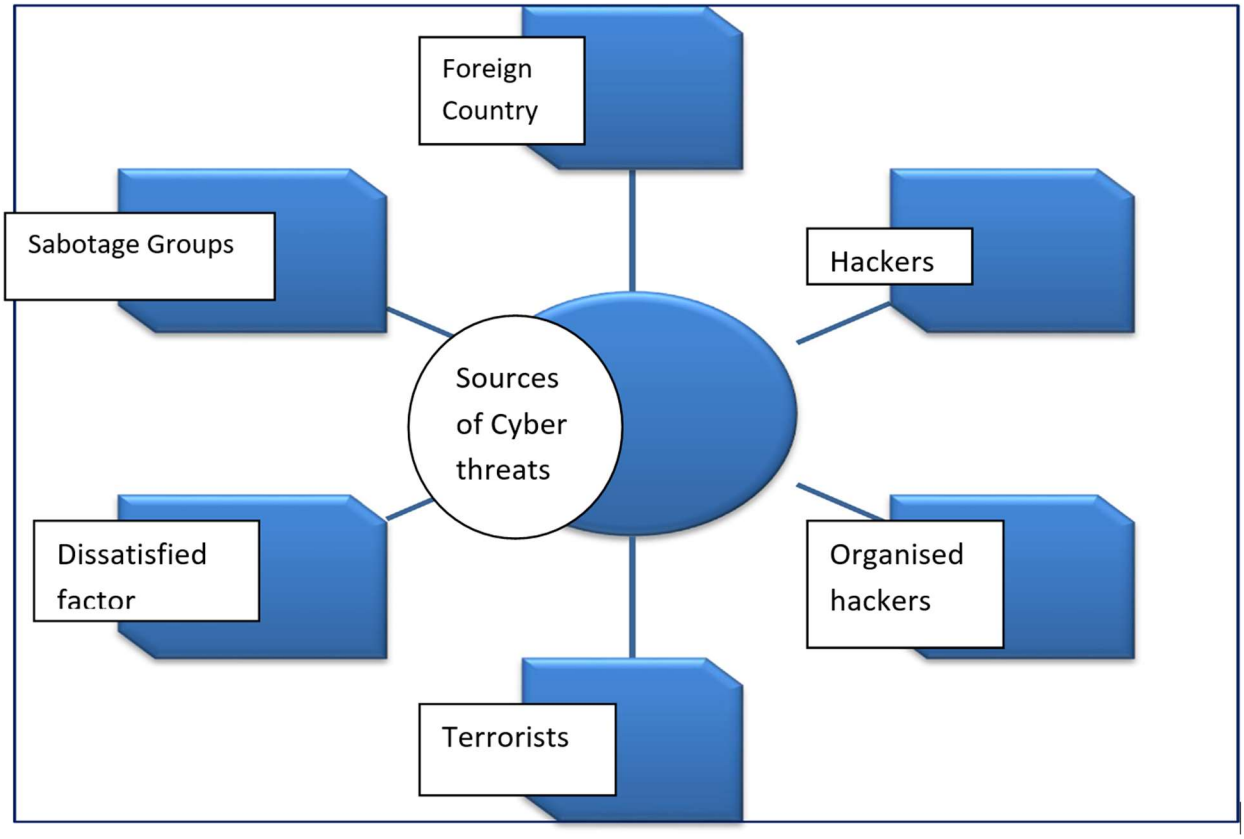


Fig. 3. Sources of cyber threats

The idea of the internet has no specialized capacity to dole out exercises to people or gatherings or associations. The essential dangers in the internet are: unfamiliar dangers, interior dangers, dangers in the store network of labor and products, and dangers because of deficient functional capacity of neighborhood powers (Al-Ghamdi, 2021). One more wellspring of assaults is gatherings who assault digital frameworks to bring in cash, and the assaults of these gatherings are expanding (Beechey et al., 2021). 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. In the mean time, another gathering (called Hacktivism) with politically thought processes assaults well known pages or email has. These gatherings generally force expanded loads on email has, and by invading the sites, they report their political messages (Solomon, 2017).

Cyberspace threats constitute a vast and intricate array of risks that target the interconnected digital realm. These threats encompass a spectrum of malicious activities orchestrated by diverse entities, ranging from individual hackers seeking personal gain to state-sponsored groups conducting cyber warfare or espionage. Cyber threats manifest in numerous forms, including malware infestations, phishing schemes aimed at extracting sensitive data, ransomware attacks disrupting operations, and sophisticated, large-scale cyber-attacks targeting critical infrastructure. The expansive nature of these threats spans across sectors, impacting businesses, governments, healthcare, financial

systems, and individual users alike. Addressing these challenges demands a proactive approach that involves constant vigilance, adaptive security measures, regular updates to defense systems, and collaboration among global cybersecurity communities to fortify digital defenses against the ever-evolving landscape of cyberspace threats.

Fear based oppressors are one more wellspring of danger that looks to annihilate, debilitating, or perniciously exploit fundamental foundation to hazard public safety, cause weighty misfortunes, debilitate the nation's economy, and sabotage public attitude and trust (Saxena and Gayathri,2021).

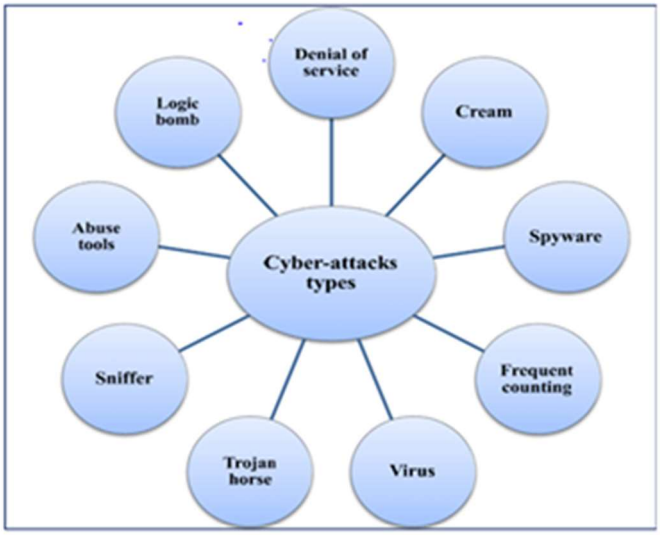


Fig. 4. Main cyber-attacks types

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 (Aziz and Amtul, 2019). 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. Botnets are likewise alluded to as electronic warriors (Kharlamova et al., 2021).

4. Cyber-security

Cybersecurity stands as the fortress defending our digital world against an array of threats. It encompasses a complex web of technologies, practices, and strategies designed to safeguard networks, systems, and data from unauthorized access, breaches, and malicious intent. In an era where our lives are increasingly intertwined with digital technologies, cybersecurity becomes the bedrock of trust and protection. It involves a proactive approach, incorporating robust defenses

like firewalls, encryption, multi-factor authentication, and intrusion detection systems to shield against evolving threats such as malware, phishing attacks, ransomware, and more. However, cybersecurity isn't solely reliant on technology; it's equally about cultivating a culture of awareness and resilience among users, ensuring they understand the risks and play an active role in safeguarding digital assets. Continual adaptation and innovation are essential in this dynamic landscape, where cyber threats constantly evolve. Ultimately, cybersecurity is a shared responsibility that spans individuals, organizations, and nations, working collaboratively to fortify our digital defenses and preserve the integrity and security of our interconnected world. (Rodríguez-deArriba et al., 2021).

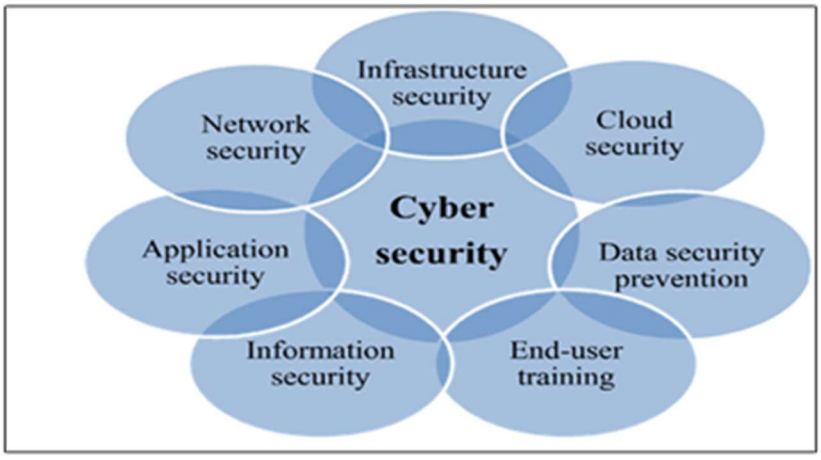


Fig. 5. Security triangle (CIA).

Fig. 6. Different types of cyber security.

Cybersecurity constitutes the bulwark shielding our digital landscape from an ever-expanding array of threats. It encompasses a vast ecosystem of technologies, protocols, and practices meticulously crafted to safeguard our networks, systems, and data from malicious intrusions and breaches. In this era of ubiquitous connectivity, where every aspect of our lives intertwines with

technology, the significance of cybersecurity cannot be overstated. It involves a multifaceted approach, deploying sophisticated tools like firewalls, encryption, and intrusion detection systems to counter a myriad of threats—from malware and phishing attacks to sophisticated cyber espionage and ransomware. Yet, cybersecurity is more than just an arsenal of protective measures; it's about cultivating a resilient mindset and a culture of awareness among users. It necessitates continuous vigilance, education, and adaptation in response to the constantly evolving threat landscape. Collaborative efforts across industries, government bodies, and individuals are pivotal in fortifying our digital defenses and ensuring the trust and security that underpin our interconnected world. Cybercrime is any unapproved action including a framework, gear or organization. Two distinct sorts of cybercrime are: Wrongdoings that utilization a framework as an objective, and the violations that a framework unconsciously assumes a part in making.

The security of any organiza-tion starts with three standards: secrecy, trustworthiness, and accessibility. These three standards are alluded to as the security triangle, or CIA, which has filled in as the norm for frameworks se-curity starting from the principal PC frameworks (see Fig. 6) (Palmieri et al.,2021).

One more limit of network protection is treatment with the developing takes part with the virtual and genuine universes of information trade. A significant test in digital protection is the shortfall of qualified word related to accomplish the work. Many individuals are at the lower limit of the vision of network safety with general abilities. The internet inclusion is a wide subject. In the accompanying article, we will survey the principal kinds of network safety. A thorough procedure covers these viewpoints and doesn't ignore any of them (Alzubaidi,2021).

5. Conclusion

In the dynamic landscape of higher education, the specter of cyber threats looms large, presenting multifaceted challenges that demand proactive cybersecurity measures. The array of cyber-attacks—from phishing schemes and ransomware to DDoS attacks and insider threats—poses significant risks to the integrity of data, operational continuity, and the trust within educational institutions. Addressing these threats requires a comprehensive approach that extends beyond technology, encompassing robust policies, continual user education, and a culture of cybersecurity awareness. While budgetary constraints, diverse IT environments, and cultural challenges add layers of complexity, prioritizing cybersecurity initiatives remains paramount. Collaborative efforts, a commitment to staying abreast of emerging threats, and a proactive stance toward cybersecurity will fortify higher educational institutions, ensuring the protection of valuable data and upholding the trust and integrity vital to academic pursuits in our digital age. The diverse spectrum of cyber-attacks, ranging from phishing scams and malware invasions to sophisticated ransomware and insider breaches, underscores the critical need for proactive protection of sensitive data and academic infrastructure. The integration of advanced technological defenses, ongoing staff and student education, and the cultivation of a security-conscious culture are imperative. Collaborative efforts, continual adaptation to emerging threats, and the fostering of a resilient

cybersecurity posture will fortify higher education institutions, ensuring the integrity of information, the continuity of operations, and the trust essential to fostering a safe and thriving academic environment in the digital era.

References

1. Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid. Energy Rep. 4, 218–225.

2. Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc..

3. Akhavan-Hejazi, H., Mohsenian-Rad, H., 2018. Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Rep. 4,91–100.

4. Al-Ghamdi, M.I., 2021. Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc..

5. Al Shaer, D., et al., 2020. Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. Eur. J. Med. Chem. 208, 112791.

6. Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Mater. Today: Proc..

7. Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats.Mater. Today: Proc..

8. Alhayani, B., et al., 2021. Best ways computation intelligent of face cyber attacks.Mater. Today: Proc..

9. Alibasic, A., et al., 2016. Cybersecurity for smart cities: A brief review. In: Nternational Workshop on Data Analytics for Renewable Energy Integration. Springer.

10. Alkatheiri, M.S., Chauhdary, S.H., Alqarni, M.A., 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. Sustain. Energy Technol. Assess. 45, 101219.

11. Alzubaidi, A., 2021. Cybercrime awareness among Saudi nationals: Dataset. DataBrief 36, 106965.

12. Amir, M., Givargis, T., 2020. Pareto optimal design space exploration of cyber–physical systems. Internet Things 12, 100308.

13. Arend, I., et al., 2020. Passive- and not active-risk tendencies predict cyber security behavior. Comput. Secur. 97, 101964.

14. Ashraf, J., et al., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities Soc. 72, 103041.

15. Aziz, A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacol. Res. 149, 104471.

16. Baig, Z.A., et al., 2017. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13.

17. Beechey, M., Kyriakopoulos, K.G., Lambotharan, S., 2021. Evidential classification and feature selection for cyber-threat hunting. Knowl.-Based Syst. 226,107120.

18. Bullock, J.A., Haddow, G.D., Coppola, D.P., 2021. Cybersecurity and critical infrastructure protection. In: Bullock, J.A., Haddow, G.D., Coppola, D.P. (Eds.), Introduction to Homeland Security, sixth ed. Butterworth-Heinemann, pp.425–497 (Chapter 8).

19. Cao, Y., et al., 2019. A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. Comput. Secur. 87,101478.

20. Cao, J., et al., 2021. Hybrid-triggered-based security controller design for net- worked control system under multiple cyber attacks. Inform. Sci. 548,69–84.

21. Chandra, A., Snowe, M.J., 2020. A taxonomy of cybercrime: Theory and design.Int. J. Account. Inf. Syst. 38, 100467.

22. Chen, J.-K., et al., 2021. Cyber deviance among adolescents in Taiwan: Prevalence and correlates. Child. Youth Serv. Rev. 126, 106042.

23. Cheng, S., et al., 2020. A new hybrid solar photovoltaic/phosphoric acid fuel cell and energy storage system; Energy and exergy performance. Int. J. Hydrogen Energy.

24. Damon, E., et al., 2014. Cyber security education: The merits of firewall exercises.

25. In: Akhgar, B., Arabnia, H.R. (Eds.), Emerging Trends in ICT Security. MorganKaufmann, Boston, pp. 507–516 (Chapter 31).

26. Dash, N., Chakravarty, S., Satpathy, S., 2021. An improved harmony search based extreme learning machine for intrusion detection system. Mater. Today: Proc..

27. Edgar, T.W., Manz, D.O., 2017. Science and cyber security. In: Edgar, T.W., Manz, D.O. (Eds.), Research Methods for Cyber Security. Syngress, pp.33–62 (Chapter 2).

28. Furnell, S., Shah, J.N., 2020. Home working and cyber security – an outbreak of unpreparedness? Comput. Fraud Secur. 2020 (8), 6–12.

29. Furnell, S., et al., 2020. Understanding the full cost of cyber security breaches.Comput. Fraud Secur. 2020 (12), 6–12.

30. Gupta Bhol, S., Mohanty, J.R., Kumar Pattnaik, P., 2021. Taxonomy of cyber security metrics to measure strength of cyber security. Mater. Today: Proc.. Hart, S., et al., 2020. Riskio: A serious game for cyber security awareness andeducation. Comput. Secur. 95, 101827.

31. Huang, J., et al., 2020. Secure remote state estimation against linear