Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/17332
DOI URL: http://dx.doi.org/10.21474/IJAR01/17332

RESEARCH ARTICLE

LEVERAGING COMPUTER SCIENCE FOR ENHANCED CYBERSECURITY

Yajat Singh
G.D Goenka Public School, Sector 48-Gurgaon.

Manuscript Info

Manuscript History
Received: 31 May 2023
Final Accepted: 30 June 2023
Published: July 2023

Key words:-
Information Technology, Cyber-Attacks, Cyber Security, Emerging Trends, Key Management

Abstract

Currently, the majority of international economic, commercial, cultural, social, and governmental contacts and activities—including those of people, non-governmental organizations, governments, and governmental institutions—are conducted online. Recently, cyberattacks and the risk of wireless communication technology have become issues for many commercial businesses and governmental institutions throughout the world. The modern society is heavily reliant on electronic technology, thus safeguarding this data from cyber-attacks is a difficult problem. The goal of cyberattacks is to financially hurt businesses. Cyberattacks may also serve military or political objectives in other circumstances. PC infections, knowledge gaps, data distribution services (DDS), and other attack vectors are a few examples of these harms. In order to protect harm from cyberattacks, numerous organizations employ a variety of measures. Researchers from all around the world have up till now offered a variety of techniques to stop cyberattacks or lessen the harm they inflict. Some of the approaches are now being used, while others are still being studied. The purpose of this study is to examine and thoroughly analyze the standard advancements made in the area of cyber security as well as to look into the difficulties, advantages, and disadvantages of the suggested approaches. The several new descendant assaults are discussed in depth. The history of early-generation cyber-security techniques are explored together with standard security frameworks. Additionally, new advancements in cyber security, security concerns, and dangers are discussed. It is anticipated that the thorough review study offered to researchers in IT and cyber security will be useful.

Introduction:-

The global economy now generates billions of dollars every year because of the enormous worldwide network that the Internet has established. Most international economic, commercial, cultural, social, and governmental contacts currently take place in cyberspace, including people, non-governmental organizations, governments, and governmental agencies. Most of the vital and sensitive information is transferred to this space or, more accurately, has been formed in this space, as vital and sensitive infrastructures and systems are either a part of cyberspace themselves or are controlled, managed, and exploited through this space (Akhavan-Hejazi and Mohsenian-Rad, 2018). The majority of financial transactions take place through this space, the majority of media activities are shifted to this space, and a sizable amount of citizens' time and activities are spent interacting in this space

Corresponding Author:- Yajat Singh
Address:- G.D Goenka Public School, Sector 48-Gurgaon.

(Priyadarshini et al., 2021). The contribution of money from internet firms to a country's Gross domestic product (GDP) has grown dramatically, and among the metrics used to gauge the level of development, online metrics account for a sizable portion. A considerable portion of a nation's material and spiritual capital is invested in this area, and a comparable portion of a citizen's material wealth and spiritual advancements are attained in or have a significant influence on this area (Amir and Givargis, 2020). However, governments now face new security issues as a result of cyberspace. The low barrier to entry, anonymity, unpredictability of the threatening geographic area, dramatic impact, and lack of public transparency in cyberspace have given rise to threats like cyberwarfare, cybercrime, cyberterrorism, and cyber espionage among strong and weak actors like governments, organized crime groups, and even individuals (Niraja and Srinivasa Rao, 2021). This makes national security in the traditional sense difficult and ineffective in this area, as opposed to cyber threats, which are distinct from traditional national security threats, which are largely transparent in nature and whose actors are governments and nations that can be identified in a specific geographical area (Sarker, 2021).

There are a number of scenarios for serious and occasionally widespread physical or economic harm, such as the function of a virus attacking an economic system's financial documents or upsetting a nation's stock market, or by sending an incorrect message, it will cause the nation's power plant to shut down and fail, or even by disrupting the air traffic control system, it will result in air accidents (Snehi and Bhandari, 2021; Ahmed Jamal et al., 2021). It will therefore be very challenging for experts to address the complex and varied dimensions and aspects of the issue and provide legal advice and analysis until governments come up with a clear definition of a cyber-attack that is accepted and favored by the international community (Cao et al., 2021).

Literature Review:-

Cyber-attacks are part of a bigger picture than what is typically referred to as information operations. One of the decision-making processes used by national institutions is information operations, which integrates the use of the key capabilities of electronic warfare, psychology, computer networks, military deception, and security operations in coordination with special support and pertinent abilities. Operations that enable computer network exploitation might also be performed with the intention of stealing crucial computer data. Trap Sniffers and Doors are useful tools for cyber espionage in such a situation (Liu et al., 2021). Trap Doors allow a third party to access software at any moment without the computer user's awareness. Sniffers are a tool for stealing passwords and usernames. In addition, there are five potential cyberwarfare scenarios. Government-sponsored cyber espionage to gather data for future cyber-attack planning, a cyber-attack to sow the seeds of unrest and uprising, a cyber-attack to disable technology and enable physical aggression, a cyber-attack to support physical aggression, and a cyber-attack with the ultimate goal of widespread destruction or disruption (cyber warfare). Encryption is one sort of cyberattack. Data may be encrypted via encryption, a reversible process that requires a key to decrypt. It is possible to combine encryption with encryption to add an additional layer of secrecy.

Cyber-attacks are activities conducted by nations to break into computers or computer networks of a nation or of other nations in order to disrupt or inflict harm (Motsch et al., 2020). In the study and criticism of this definition, it may be claimed that the three criteria—the attacker, the attack's goal, and its intention—have been applied without taking disruption types into account (Cao et al., 2019). Additionally, only nations are cited when referring to the assault's perpetrator in general; nevertheless, if an attack occurs in a situation and a region that is under the legal control and jurisdiction of a country (such as a network in cyberspace controlled by a country), both persons and If private and non-governmental organizations take action against a third country.

Computer systems that have been subjected to digital assaults appear to be operating normally but actually create and issue false replies (Quigley et al., 2015). This definition of a cyberattack really leaves out a broad variety of possible risks to the national security of a nation whose cyber infrastructure has been attacked but has not yet reached the intensity and threshold of significant assaults. The target nation's computer systems and networks are actually susceptible to damage from these threats. Any definition of a cyber-attack that does not include the aforementioned would thus be insufficient and lack the requisite comprehensiveness (Damon et al., 2014; Shamel et al., 2016).

Findings and Discussions:-

Every business and organization's infrastructure must take cyber security seriously. In conclusion, a business or organization that focuses on cyber security has a greater chance of success because it can better defend its

customers' and employees' personal information from outside threats. Abuse is committed by businesses and rivals of consumers and people. In order to start and grow, a business or organization must first and foremost offer this security. Practical ways to safeguard data, networks, and information from internal or external threats are included in cyber-security. Professionals in cyber security safeguard computers, servers, intranets, and networks. Cybersecurity ensures that only authorized users may access the data. Knowing the many sorts of Network Security: Network security guards against hackers and viruses, which can damage a computer network. Network security is a collection of tools that allow organizations to protect computer networks against viruses, coordinated attacks, and hackers. Threats are essential for effective defense.

Cybercrime is any unauthorized activity involving a system, equipment or network. Two different types of cybercrime are: Crimes that use a system as a target, and the crimes that a system unknowingly plays a role in creating. Any unlawful behavior involving a system, piece of technology, or network is considered a cybercrime. Cybercrime may be divided into two categories: crimes that target systems and crimes that systems unintentionally contribute to. demonstrates the techniques used by hackers the most. Any organization's security must start with three guiding principles: confidentiality, integrity, and availability. The security triangle, often known as the CIA, is made up of these three ideas and has been the gold standard for system security since the invention of computers. According to the confidentiality concept, only authorized parties should have access to sensitive data and operations.

A new vulnerability to hacking and cyber-attacks is however created by the deployment of an online system. Organizational decision-makers need to take assaults' potential impact on performance into account when planning their agenda. The security of online apps is considered by some of the top new hackers to be the weakest place for assaulting an organization. Excellent encryption is the first step towards application security. Every plan needs to be individually created and used for every firm. Information hacking and intrusion are made less likely in this way. Cybersecurity is getting more difficult. A "security perspective" on how cyber-security functions is necessary for organizations. As a consequence, to stay one step ahead of hackers, you must constantly have good security. Investment in cyber-security systems and services is growing as a result of rising security endeavors. A new vulnerability to hacking and cyber-attacks is however created by the deployment of an online system. Organizational decision-makers need to take assaults' potential impact on performance into account when planning their agenda. The security of online apps is considered by some of the top new hackers to be the weakest place for assaulting an organization. Excellent encryption is the first step towards application security. Every plan needs to be individually created and used for every firm. Information hacking and intrusion are made less likely in this way. Cybersecurity is getting more difficult. A "security perspective" on how cyber-security functions is necessary for organizations. As a consequence, to stay one step ahead of hackers, you must constantly have good security. Investment in cyber-security systems and services is growing as a result of rising security endeavors.

Conclusions:-

In the third millennium, one of the most significant sources of power is cyberspace and related technology. Since governments have so far divided the game of power among themselves, other actors—such as private companies, organized terrorist and criminal groups, and individuals—must now be involved, although governments still play a significant role in this. These other actors include private companies, organized terrorist and criminal groups, and individuals. Naturally, the national security of governments will not be compromised by this phenomenon. There are several ways to analyze this effect. Security is the first idea. Military concerns and internal and external boundaries cannot be used to define national security today. The second is that cyber dangers no longer have a geographic component. Military threats in the past had a particular area. Consequently, it wasn't challenging to handle, at least in terms of identification. The size of the risks that cyber threats offer comes in third. These attacks are unpredictable, multifaceted, and extremely damaging since they affect infrastructure and sensitive networks. Fourth, governments alone are not sufficient to combat them, and effective and bilateral cooperation between governments and the private sector, which has common interests in dealing with them, is necessary. These threats cannot be contained by conventional means alone, such as the use of military and police force. He demands when such threats are made. Fifth, as the preceding point demonstrates, cyber risks are not just a problem for governments; people and businesses are also susceptible to their negative effects. Sixth, the numerous theoretical approaches in international relations whose ideas are centered solely on government are easily missed or misunderstood since security in the digital age is not just governmental.

References:-

1. https://www.mooc.org/blog/cybersecurity-and-computer-science-whats-the-connection
2. https://www.sacredheart.edu/academics/colleges--schools/school-of-computer-science--engineering/computer-science--cybersecurity-blog/
3. https://www.studyinternational.com/news/strengthening-technology-through-computer-science/
4. Fees, R. E., Da Rosa, J. A., Durkin, S. S., Murray, M. M., & Moran, A. L. (2018). Unplugged cybersecurity: An approach for bringing computer science into the classroom. International Journal of Computer Science Education in Schools, 2(1), 3-13.
5. Tyagi, A. K. (2016). Cyber physical systems (cpss) â [euro]" opportunities and challenges for improving cyber security. International Journal of Computer Applications, 137(14).
6. Ayofe, A. N., & Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29(6).