Empirical Study on Research Trends and Challenges in Cyber Security and Governance

P.ASHOK KUMAR , MCA.,MPhil
Department of Computer Applications
AVS College of Arts and Science
Salem, India
ashokasvs@gmail.com

Dr. M. RAMALINGAM,
MSc.(CS).,M.C.A.,Ph.D
Associate Professor
Gobi Arts & Science College(Autonomous),
Gobichettipalayam-638453
ramsgobi@gmail.com

A. KESAVMOORTHY
Department of Computer Science
K.S.Rangasamy College of Arts and Science
Tiruchengode, India
kesavamoorthy3909@gmail.com

***Abstract* — The buzz word "cyber security" covers the entire facts of protecting a company's resources, workforce, and maneuvers from online or web related hazards. A diversity of computer-generated protection resolutions are needed to diminish industry virtual hazard as virtual attacks become more recurrent and complicated and community networks become additional problematical. The availability, integrity and confidentiality of data are characteristically the focal point of cyber safety measures. Business services includes user authentication, accountability, reliability and authorization are maintained by these kinds of elements. The comprehensive cyber security strategy called cyber security authorities integrates with secretarial maneuvers and guards adjacent to the interruption of operations conveyed on by virtual threats or attacks. Cyber security governance characteristics include: frameworks for accountability, hierarchies for making decisions. The information technology sector should obtain the following six steps to help their own organization's grow and sharpen their cyber security governance contents. Establish the current state; Create, review and update all cyber security standards, policies and progression; Approach cyber security from an enterprise lens; Increase cyber security awareness and training related activities to users; Cyber-risk analytics: How are different kinds of threats designed and risks contextualized and evaluated? And finally Monitor, measure, analyze, report and improve. The development and maintenance of cyber security capabilities that guarantee the secure use of digital services falls squarely on the shoulders of governments and businesses. This current trends and challenges related to the cyber security and its governance related activities are discussed in this empirical study.**

Keywords—Cyber security, Governance, Cyber-risk Analytics, Cyber Attacks, organizational Operations.

I. Introduction

The observation of defending networks, connected and non connected computers, multiple servers, different mobile gadgets, electronic devices, and data of information from intimidating attacks is recognized as cyber security. It is often referred to as electronic information security or information technology security [1]. The major objective of a cyber-attack is to crooked the embattled asset or attain admin-like right of entry to it so that the accumulated data or information possibly will be accessed or connected utilities might go wrong. The figure one illustrates the different types of cyber attacks.

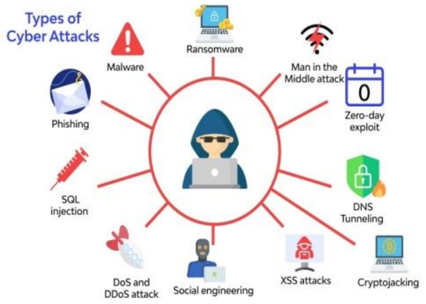

Figure.01. Types of Cyber Attacks

Man-in-the-middle attack

By using the MitM technique, the threat actor is introduced as a trustworthy resource between two entities, such as different types of computer systems and a multiple servers or an inter-connected server and a web deployed applications. The assault becomes a component of data or information exchange and other procedures with the forced introduction between two parties and takes important information.

DoS and DDoS attack

By delivering an excessive number of access requests, Denial of Service (DoS) and Distributed Denial of Service (DDoS) prevent verified resources from accessing a certain system or website. For instance, an attacker can bombard a company's CRM software with access requests in order to keep it busy and prevent real professionals from using it when they are in need. It mostly serves as a planning tool for future, more destructive attacks.

SQL injection

These attacks are carried out via malicious SQL-based programmes that are added to the weak systems and apps. A successful SQL injection preserve to gather the query related results, issue fresh commands to the computer systems, and carry out illegal acts after being introduced.

Zero-day exploit

This phrase refers to cyber attacks that go unreported for weeks or even months at a time. Zero-day exploits often work by exploiting any flaws in hardware or software.

Generally speaking, 0-day attacks start out mildly and persist a longer period of time.

DNS Tunneling

It is not unusual for cyber attacks to take advantage of DNS tunneling, a well-known transactional mechanism. Attackers can take advantage of these and steal vital information. Organizations must take extreme precautions to avoid it because the related protocol interacts with the application's data exchange operations.

Phishing

Phishing attack is a type of cyber security attack which uses to compromised emails to steal sensitive data and causes significant annoyance. To entice the target of a cyber assault, threat actors may send enticing emails with messages similar to "you have won a prize," "you got an offer," "a loan is approved," and numerous other kinds. These emails will invite the target to made click on a specific linkage and disclose information which includes credit card numbers, bank account information, CVV data, and its related many other things. The e-mails are so expertly written that it appears they are from reliable sources. Nearly 50% of all cyber attacks that occur worldwide involve phishing.

Malware

The goal of a malware cyber attack is to steal information from the targeted system or cause it to entirely malfunction. These assaults make use of a variety of software, including Trojan, Remote Access Trojan, worms, and ransomware.

XSS attacks

XSS, also known as cross-scripting attack, is essentially a safety measures flaw that affects the entire online o web application. If an XSS attack is successful, the attacker will be able to add client-side scripts to the beleaguered web application or online page. And the exploit is frequently used to get around admission control restrictions placed on an online or web application.

Social engineering

Social engineering is a one type of cyber-attack that depends on manipulating the target's mind. Unlike other cyber-attacks, it requires special knowledge to manipulate people, exploit their emotional tendencies, and track personal or sensitive data. The most frequent application of this method, which has a incredibly elevated accomplishment rate, is intrusions.

Ransomware

Ransomware attacks are a subset of cyber-security attacks that threaten the victim with leaking or publishing sensitive information in the civic province if the demanded payoff is not compensated. The hacker infects the victim's system with ransomware at the start of the attack, which decrypts the victim's data and sends it to the hacker. Phishing, adware, and USB sticks are some of the most popular methods for spreading ransomware.

Crypto jacking

Crypto jacking, one of the most recent and bothersome cyber attacks, targets only bit coin possessors. Attackers expand admittance to user's assets and begin mining crypto currency. The wherewithal and network of the victim will now be used to pay for this resource-intensive task, with the gain going to the intrusion.

Why are there cyber attacks?

A cyber-attack may have any number of motives, including the theft of data or money. The following are some of the main causes for conducting a cyber-attack. The majority of cyber attacks are designed to bring in money. A successful cyber attack, at the very least, has the potential to benefit the attacker in many ways.

The acquisition of business intelligence is the second primary motive for a cyber attack. Hackers strive to take control of a certain organization or enterprise to demonstrate their superiority, and they do this through obtaining passwords, sensitive information, access information, and its related other information.

Hacktivism is a genus of cyber security assault that focuses on raising people's opinionated consciousness. For instance, Wiki Leaks has already attacked political organizations online in order to expose internal conspiracies, corruption, and many other problems. Some cyber attacks are motivated by resentments that an individual or group has towards them. For instance, a worker might steal data if the proper promotion wasn't given to them.

White-hat hackers, who engage in moral hacking or hacking with good intentions, launch cyber attacks to expose hidden hazards or test an organization's defenses. Sometimes a cyber-attack is carried out exclusively because information was easily accessible or the user end is ignorant of proper security procedures. They take advantage of the chance to put their abilities to the test, learn the new hacking technique, and demonstrate their superiority [2].

It's challenging to stay safe in a world when more than 440,000 businesses are impacted by cyber-attacks. Numerous large and small businesses have fallen prey to cyber attacks. This paper discussed about the different existing methods which are already suggested to prevent and avoid the users to become a prey to the attackers in online.

II. Fundamental Concepts

Cyber security attacks are component of a bigger depiction than what is naturally referred to as data or information operations. Data or Information operations pooled the utilize of the major components of electronic conflict, psychological, system or computer network, armed services deception, and security related operations in association with precise support and relevant talents in order to infiltrate, end, obliterate, or take control human decisions and it is one of the nationwide organizations' decision-making measures [3]. Figure 02 explains the composition of the cyber security attacks and the fundamental definitions and ideas of cyberspace are laid down in table one.

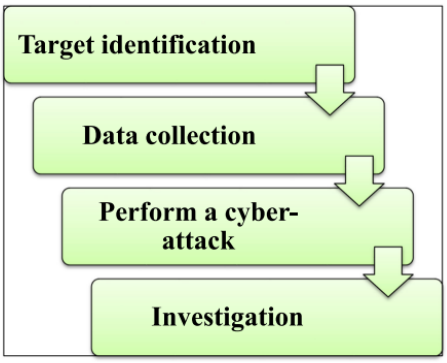

Figure.02. Anatomy of a Cyber Attacks

Cyber warfare's effects could lead to the following:

1. The conquers of the political organization or a grave hazard to nationwide security.
2. Instantaneous start of corporeal combat or preparations for physical combat that will take place soon.
3. Calamitous loss of status or damage to the nation's standing abroad.
4. Calamitous corrosion or destruction to the nation's opinionated and financial relations.
5. Large-scale individual casualties or a hazard to the physical condition and protection of the public.
6. Prevalent commotion to the nation's administration.
7. Obliterating the public's confidence or national, ethnic, or religious beliefs.
8. Extensive impairment of the functionality of countrywide cyber or virtual assets.

TABLE.01. Basic meaning and perceptions of cyberspace

Term	**Definition**
Cyber space	Networks that are unified for the rationale of producing, dispensation, storing, retrieving, and exploiting data include IT infrastructures, communiqué networks, PC, entrenched processors, key manufacturing controllers, and the communication between these surroundings and people.
Cyber capital	A crucial cyber system, a crucial piece of a country's infrastructure, an important piece of information, or citizens of a country.
Cyber-vulnerability	A weakness in a talent, security protocols, internal controls, or execution of that nationwide cyber quality is referred to as a vulnerability that can be browbeaten or stimulated by domestic or outside threats to demeanor cyber conflict.
Cyber threats	Every occurrence that has potential to undermine information systems' missions, errands, descriptions, countrywide cyber assets, or employees through unauthorized access, information or data deletion, disclosure, information manipulation, or obstruction of (disruptive) service delivery.
Cyber hazard level	Nationwide cyber or virtual assets at the intercontinental, nationalized, institutional, unsophisticated, critical, and critical stages of infrastructure are all susceptible to cyber threats.
Probability of cyber or virtual threats	Elevated (probable), Elevated (extremely likely), stumpy (very unlikely), and extremely stumpy (imminent).
Intensity of cyber threat	Very Elevated (tragedy), Elevated (catastrophe), restrained (major security incident), stumpy (security incident), and very stumpy (security incident) are the dissimilar types of incidents.
Cyber attack	The phrase "cyber-attack" refers to several unauthorized cyber or virtual demeanor projected to infringe the security guiding principle of a cyber-asset and consequence in damage, disturbance of services, or admittance to information or data related to the specified nationwide cyber or virtual asset. Cyber-attacks are also definite as the premeditated utilize of a cyber-weapon against information or a data system in a method those results in a cyber or virtual related incident.
Cyber-weapon	An arrangement created and contrived to harm the functionality of additional virtual or cyber systems is known as a cyber weapon. To stop service attacks and disseminated service, these systems comprise bot networks, logic bombs, cyber susceptibility utilization software, and traffic generating systems.
Cyber-warfare	It is the most serious and sophisticated form of cyber or virtual attack (cyber procedure) that targets a nation's cyber interests and has the most terrible consequences.
Cyber warfare origin	The cyber strength of the assailant nation or parties affiliated with the assailant states, as well as any cyber weapons these forces control or choose to abandon
Cyber defense	Using all of a nation's exposed virtual and non-cyber facilities to produce preclusion, avoidance, discovering, and an effective, restraint reaction to several cyber or virtual attack.
Cyber-biome	The creation of a inhabitant and self-motivated cyber or virtual environment that supports a country in many dissimilar disciplines is known as a "cyber biome."
Virus	It is a self-replicating method or programme that increased to other files and programmes by making copies of it and has the potential to break programmes. A computer or system virus behaves similarly to a real virus, which increased by reproducing inside of host body cells.
Hacker	a person who breaks into a system without authorization or one who expands their altitude of admittance to information or

	data in order to peruse, duplicate, reinstate, erase, or otherwise harm it.

Additionally, only nations are cited when referring to the attack's perpetrator in general; nevertheless, if an attack occurs in a situation and a region that is underneath the legal power and authority of a nation (such as a network in cyberspace controlled by a country), both individuals and There should be a vacuum in the legal protection against such assaults if non-governmental and private organizations commit acts of aggression alongside a third nation because they essentially descend beyond the purview of the aforementioned description and are not included [4]. Given this context, it can be argued that the aforementioned explanation is essentially insufficient, leaves out a major segment of attacks carried out by commercial and non-governmental associations, and also creates a fissure in the literature.

III. Cyber-security

Every big business and multinational organization's infrastructure must take care of cyber security related issues in seriously manner. In conclusion, an enlarged business or developing organization that focuses on cyber or virtual related security has a greater probability of accomplishment because it can improve to protect its customers' and employees' individual and private information from exterior threats. Mistreatment is dedicated by businesses and rivals of clientele and persons. In order to commence and cultivate, a company or association must primary give this fortification in the greatest potential method [5].

Convenient procedures to preserve data or information, networks, and data or information against interior or exterior threats are incorporated in cyber-security. Leading Professionals in cyber safety measures safeguard personal computers, multiple servers, dedicated intranets, and widespread networks. Cyber safety measures makes ensuring those only publics with authorization can admittance the information or data.

The various forms of cyber security are shown in Figure.03. Network safety measures guards alongside attackers and malware programes, which can harm a computer network. Network security is a collection of tools that allow organizations to protect their computer networks against viruses' related attacks, coordinated related attacks, and also from the hackers.

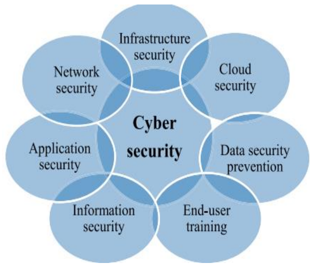

Figure.03.Cyber Security

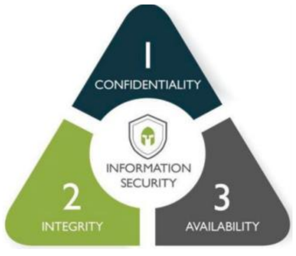

Figure.04.Information security types

Application security - By via hardware and software, the system is protected from exterior hazards that could impede the development of normal or web related applications. Information or data security guards alongside unlawful admittance, revelation, exploitation, unlawful alterations, and removal of either physical and digital data or information. Operational security refers to the measures and multiple choices taken to handle and protect data or information. For occurrence, client rights for system admittance or procedures that sketch the timing and locality of data storage and sharing. A cloud safety measure avoids hazards from on-site attacks by conservation information on the cloud (based on software) [6]. Client education: Discusses the unpredictable aspects of cyber security, primarily public. A bug could inadvertently pierce the security classification from anybody and showing the client, how to eradicate distrustful. Any organization's commercial security chart should concentrate on concerns like e-mail attachments, connecting to unidentified USBs, and additional decisive ones.

Any Multinational companie's security should start with three directing principles: confidentiality, availability and integrity [7]. The security triangle, often identified as the CIA, is ended up of these three doctrines and has been the gold standard for computer system security since the invention of computers and the same illustrated in the figure.04.

According to the privacy concept, only official parties must have admission to sensitive information or data and its related operations, Military or armed force secrets, for illustration (Confidentiality). Only certified populace and possessions are allowed to modify, insert, or eliminate sensitive data or information and functions, according to the principles of truthfulness. Example: Integrity, a database contains inaccurate data entered by a user. According to accessibility principles, computer systems, related services, and information or data have to be readily accessible upon demand within determined limits based on Service Level Agreement - service level of Availability.

The finest computer-generated safety measures techniques diverge from the previously traditional guiding principles. This straightforward protection can be conquered by any experienced hacker. A Cyber safety measure becomes increasingly multifaceted as an industry expands [8]. The handling of the expanding information or data exchange participation involving the actual and implicit worlds is an additional limit of cyber safety measures. Then be deficient in of capable workers to execute the job is a significant obstruction in cyber safety measures. A lot of persons with universal capabilities are at the foundation end of the cyber-security continuum. The area of cyberspace exposure is wide-ranging [9].

The security measures of online or virtual application are measured by several of the top novel hackers to be the weakest consign for assaulting an association. Outstanding encryption is the primary step towards application or web application security. Every arrangement needs to be independently crafted and used for each organization. Information or data hacking and interruption are complete less likely in this way. Cyber security measures are getting more complicated. Businesses should have a "security perspective view" on how cyber security functions and how it will benefit the business [10]. As a consequence, to reside one step forward of hackers, users must constantly have high-quality security measures. Investment in cyber-security systems and its related services are increasing as security companies cultivate. Trend Micro, Cisco, and McAfee are some of the three main multinational businesses involved in this digital industry.

The nation's cyber policy is now a component of its countrywide security policy. Even if users assume that a nation's cyber fortification stratagem is in line through the State Department's or the country's economic strategy, these kinds of laws and strategies don't have the equivalent level of authority as the establishment. In actuality, policy is urbanized and disseminated in reports and addresses through conversation of various issues [11]. To direct and make pronouncements on rules and regulations, policies are developed. The policy itself has nonentity to do with laws, rules, regulations and ordinances. At their level best, laws, contracts, and norms provide as intellectual and efficient policies. But without emergent a cyber-security policy, commands, laws, rules, and set of laws-regulations can be supplied for cyber-security enforcement.

Because penalty will be applied in anticipation of the aberrant sector is lock down, different sectors of a corporation are expected to tolerate by the rules. For instance, human source, communal, or estimating policies may be designed so that any violation of the announcement requirements results in the closure of the appropriate section. Central managers grant sustain for procedures like employing human resources or recording operating cost. They are also predictable to incorporate unrestrained policies into departmental proceedings and endow with indicators for measuring guiding principle compliance at the departmental intensity. Any organizational or business subdivision in the communal sector is subject to supremacy restrictions.

The cyber security policy leaves the determination of data risk up to the management, who possibly will desire to slash operating cost by outsourcing the office's information stream and engaging external contractors to accomplish information psychoanalysis. Perchance the identical superior seeks to cut costs by avoiding examination [12]. A situation like this arises when information duties are assigned to someone who is not a security expert incorrectly, or it could be that the risk is inherent in the organization's culture. In any scenario, task separation is crucial. Owing to the reality that cyber-security procedures have not highly developed as greatly as secretarial or individual resource pointers, these situations become more complex and challenging.

IV. Conclusion and Future Scope

In the third millennium, the majority significant sources of control are cyberspace and its correlated technologies. While administrations have so extreme alienated the fixture of influence amongst themselves, supplementary factors – Which includes classified businesses, prearranged revolutionary team and illegal grouping and persons – must currently be involved, even though governments silently playing a momentous task in this things. Obviously, the countrywide safety measures of governments will not be negotiated by these kinds of occurrences.

There are a variety of traditions to investigate this consequence. The primary is the thought of protection. Nationwide protection currently is threatened by the opportunity of citizens' superiority of existence falling, not by military or armed concerns or the continuation of domestic and peripheral boundaries.

The subsequent is that virtual hazards no longer have a geographic constituent. Military or legally armed threats in the precedent had an exacting region. Accordingly, it wasn't demanding to handle, at least in terms of recognition. The dimension of the risks that virtual threats pretense comes in next level. For the reason, that they distress fragile networks and communications, these threats are irregular, versatile, and have am elevated prospective for damage.

Fourth level, governments unaccompanied are not adequate to warfare with them, and effectual and two-pronged collaboration between government departments and the private division, which has widespread welfare in dealing with them, is compulsory. These kinds of threats cannot be controlled by conservative means alone, such as the utilizing of military or armed and police strength.

Fifth part, as the preceding point expresses, computer-generated risks are not presently a predicament for governments; public and different kinds of businesses are also vulnerable to their unconstructive effects.

Finally, the abundant hypothetical approaches in intercontinental relations whose theories and thoughts are based solely on official departments or government are easily neglected or misunderstand since safety measures in the digital era is not just legislative.

These are taken into consideration, to prevent cyber war between corporations and attackers, cyber security will be expanded in the future. The IoT is one of the various digital scenarios where the cyber space is growing. So, in order to thrive in this digital age, policy-based cyber security is required.

References

[1] Jie Cao, Da Ding, Jinliang Liu, Engang Tian, Songlin Hu, Xiangpeng Xie, “Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks”, Information Sciences, Volume 548, February 2021, 69-84.

[2] Obi Ogbanufe, “Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity”, Computers & Security, Volume 108, September 2021, 102340.

[3] Steven Furnell, Jayesh Navin Shah, “Home working and cyber security – an outbreak of unpreparedness?”, Computer Fraud & Security, Volume 2020, Issue 8, August 2020, 6-12.

[4] Seema Gupta Bhol, JR Mohanty, Prasant Kumar Pattnaik, “Taxonomy of cyber security metrics to measure strength of cyber security”, Materials today: Proceedings, Volume 80, Part 3, 2023, 2274-2279.

[5] Yunxiao Zhang, Pasquale Malacaria, “Bayesian Stackelberg games for cyber-security decision support”, Decision Support Systems, Volume 148, September 2021, 113599.

[6] Xiaoxue Liu, Jiexin Zhang, Peidong Zhu, Qingping Tan, Wei Yin, “Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game”, Computers & Security, Volume 102, March 2021, 102138.

[7] Dr. Chat Le Nguyen, Dr. Wilfred Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'", Computer Law & Security Review, Volume 40, April 2021, 105521.

[8] Tierui Zou, Arturo S. Bretas, Cody Ruben, Surya C. Dhulipala, Newton Bretas, "Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks", Electric Power Systems Research, Volume 187, October 2020, 106490.

[9] Onur Kemal Tosun, "Cyber-attacks and stock market activity", International Review of Financial Analysis, Volume 76, July 2021, 101795.

[10] Lei Ma, Ying Zhang, Chunyu Yang, Linna Zhou, "Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: The input-to-state stability", Journal of the Franklin Institute, Volume 358, Issue 12, August 2021, Pages 6309-6325.

[11] Bilal Alhayani, Sara Taher Abbas, Dawood Zahi Khutar , Husam Jasim Mohammed, "Best ways computation intelligent of face cyber attacks", Materials Today: Proceedings, 2021.

[12] Stephen Hart, Andrea Margheri, Federica Paci, Vladimiro Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education", Computers & Security, Volume 95, August 2020, 101827