International Journal in Management and Social Science
Volume 09 Issue 11, November 2021 ISSN: 2321-1784 Impact Factor: 7.088
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

ANALYSING THE PERSPECTIVE OF CYBERCRIME AND CYBER SECURITY AND ITS LIMITATIONS

RAYEES FATIMA
RESEARCH SCHOLAR, SUNRISE UNIVERSITY ALWAR

DR. JITENDER RAI
PROFESSOR, SUNRISE UNIVERSITY ALWAR

ABSTRACT

The focus of this research is on the importance of cyber security for state, municipal, and national governments, which store and use vast amounts of sensitive information about their constituents. When terrorists get into government databases and steal classified information, it poses a serious danger to the whole country. As a result, cyber security is not only crucial for government agencies but might be an invaluable resource for the country as a whole. Based on the reviewed literature and current state-of-the-art in the cyber world, it is clear that optimizing the problem of security management in the cyber world for solutions to minimize cyber loss and provide more security is necessary for the visualization of the cyber world as a single entity that can be managed more easily and efficiently. The scope of cyber security has expanded beyond the protection of corporate information technology to include the safety of the Internet and other digital networks. The growth of IT and related services is crucially dependent on cyber security. Improving cyber security and safeguarding critical data infrastructures is key to the security and prosperity of countries. Cyber systems have become integral to every facet of modern life, from trade and banking to healthcare and energy production to the delivery of news and entertainment to the conduct of military operations. The results of this study also show how popular concern for personal data and privacy has grown.

Keywords: -Cyber, Security, Crime, Cyber space, System.

I. INTRODUCTION

In the twenty-first century, the Internet plays a crucial role in making people's lives easier in terms of time management and productivity. It's become essential to human survival in the modern era. All throughout the globe, governments, businesses, and regular people have rediscovered the web's useful resources. The Internet has ushered in a new era of instantaneous communication, electronic money transfer, data sharing, easy access to government services, and many other innovations. Internet use is universally acknowledged. On the other side, an increase in cybercrime has been linked to Internet use. Consequently, cyber security plays a crucial role in understanding the severity of these threats and implementing countermeasures.

According to the PwC survey study, cybercrime ranks second in the financial industry in terms of economic crime, accounting for 38 percent. One-third of data breaches, according to a study published by the Verizon report, have harmed the financial institution. Most businesses now use cloud computing because it reduces costs. However, as enthusiasm for "cloud computing" grows, so do concerns about data loss, privacy invasion, and security breaches.

II. CYBERSPACE

In 1990, the World Wide Web was introduced, and since then, most communities have gone digital and been connected in cyberspace. Since 1991, an enormous number of individuals have joined, and cyberspace has spread to permeate all facets of the contemporary world. Cyberspace encompasses a wide range of concepts—from software and hardware to the Internet and information to linkages and servers and personal computers to the relationships between individuals, groups, nations, and society. Therefore, cyberspace is mostly an abstract concept that is difficult to pin down. Cyberspace may have a significant role in today's advanced societies. Cyberspace is where people, societies, and even military meet, mingle, and form themselves. From 2000 to 2010, the number of people using the Internet globally grown from 360 million to more than 2 billion Cyberspace will become the area upon which everyday life is dependent around the world as Internet uses and networking continue to increase.

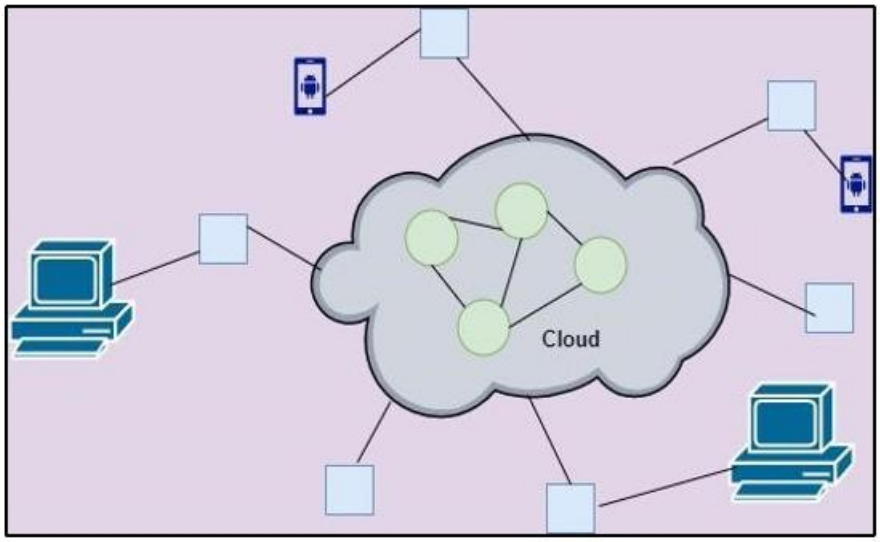

Figure 1.1 Architecture of Cyberspace

The lightning-fast pace of events in cyberspace is one of its defining features. Companies may quickly and easily move goods and resources throughout the world via cyberspace. Cyberspace is not only a vital part of the global economy because it facilitates trade across diverse sectors,

but also because it generates significant economic activity. Business models, technological advancements, the proliferation of open dialogue, and the emergence of fresh social networks have all benefited from the infrastructure that the Internet provides. Cyberspace of commercial management systems, and information technology are vulnerable to interruption or cyber exploitation, putting at risk the safety and effective functioning of key infrastructure including energy, banking and finance, transportation, communication, and protection.

III. CYBERCRIME AND EXPLOIT

Cybercrime does not fit the global norm for criminal activity. The Information Technology Act defines it as any crime committed using or facilitated by a computer, the Internet, or any other type of technology. The prevalence of cybercrime in contemporary India is astonishing. Not only have criminals caused substantial damage to citizens and the government, but they are also adept at remaining anonymous. By and large, technically savvy criminals do a subset of their illicit actions online. Taking a broader view, it is generally said that cybercrime includes any illegal conduct when a computer or the internet is used as a tool, a target, or both. It is possible to find judicial interpretations of the phrase "cybercrime" in a small number of decisions made by Indian courts, although the concept is not defined in any act or legislation that has since expired from the Indian Legislature. Rapid advancements in the use of computer-related alternative allied technologies are promoting more customer comfort. It's a never-ending, incomprehensible sea of media. Despite all the good things the internet can do for us, it also has certain drawbacks.

IV. CYBER SECURITY

First, we explain some key terms and provide a brief overview of how cyber security relates to information security. Finally, the problems with cyber security are discussed.

Cyber Security vs. Information Security

- **Cyber security**

The goal of cyber security is to prevent unauthorized use of an organization's computers, data, and network by implementing a set of procedures, policies, and technological safeguards. The purpose of this safeguarding is to protect the company's data, network, and good name against attack.

- **Information Security**

Information security prevents data, both digital and physical, from being intercepted, altered, destroyed, or recorded without authorization. If a company is only now putting together a security plan they should start with Information Security as it is the foundation of the field.

Security Concept

Cyber security refers to the practice of limiting access to data and information systems by proper procedural and technical safety measures. When discussed in the open, concepts like protection, data sharing, intelligence collecting, and surveillance are often mistakenly grouped along with cyber security.

A person's ability to control who has access to their information via third parties is closely linked to their level of protection. Therefore, adequate cyber security will assist to safeguard privacy in the electronic realm; yet, data supplied to aid cyber security efforts may occasionally include private information that at least some observers would think to be private.

The goal of cyber security is to prevent unauthorized access to, or use of, a computer system or network. However, if directed towards possible cyber-attack sources, such actions may serve to positively affect cyber security. Also crucial to cyber security is surveillance in the form of various observations of data flow inside a system.

Management of Cyber Security Risks

There are three factors that contribute to the danger posed by every attack: vulnerabilities, threats, and impacts. Successful cyber security is said to begin with risk management for information systems.

- The danger is a person, thing, or substance that poses a continuing risk to the asset. Something that takes advantage of a weakness in order to cause damage or destruction to an asset.

- Vulnerability may represent a security gap or weak spot. Impact a successful attack can trade off the confidentiality, integrity, and availability of an ICT framework and the data it handles.

- Vulnerability A flaw or weakness in an information asset, safety technique, technical design, or control that a risk may exploit intentionally or unintentionally to break the security system.

Various measures may be taken to lessen the likelihood of cyber assaults, including

- Expelling the threat source
- Addressing vulnerabilities by hardening ICT
- Reducing negative consequences by repairing broken systems and restoring normal operation.
- The utmost efficacy of cyber security is within your reach, and we've outlined six ways to get you there. These six stages are essential for every cyber security program.

Objective of Cyber Security

It's a theoretical framework meant to direct protocols for keeping sensitive data secure.

- **Confidentiality:** The concept is equivalent to that of private quarters. Security measures are put in place so that private data may only be accessed by those who need it.
- **Integrity:** The term "data integrity" refers to the process of ensuring the accuracy and consistency of data throughout its lifespan.
- **Availability:** In this context, "data" means ensuring that only authorized users may access the information when it is needed.

Challenges of Cyber Security

There must be rigorous security measures in place to protect the data. All information is now stored digitally, or "in the cloud," and this is the world in which we now reside. Users may feel secure interacting with friends and family on social networking sites. For domestic users, the next step would be to attack a social networking platform and steal personal information. A person should take all the required safety precautions not only while using social networks, but also when conducting financial transactions.

V. LIMITATION OF CONVENTIONAL CYBER SECURITY TECHNIQUE

Once systems are susceptible to coordinating and malevolent assaults, traditional techniques can no longer be maintained. If any hardware or software component of the system is constructed to convey the internal data to outside the system or entice attackers on purpose, conventional information security execution will be of little use. Proper inspection of network components,

observation of supply chain stages, and history check of network component providers might limit this form of backdoor access. Due to the slowness of the detecting method, there are still significant limitations on precision or throughput. The traditional hashing strategy for password security creates two types of problems:

1) Brute Force Attack

2) Salt Collision

Brute Force Attack

The length of every possible combination of characters is cut in half. While effective in breaking the password, this type of attack is computationally intensive and often the least competent in terms of hashes cracked per processor time.

Salt Collision

When two passwords are encrypted using the same salt value, this is called a salt collision. In the event of a dictionary attack, the intruder sorts the hashed and salted passwords in accordance with the candidate passwords from a dictionary.

VI. CONCLUSION

Cybersecurity now encompasses not just the protection of IT systems inside businesses, but also larger digital networks, which include both cyberspace itself and its essential supporting infrastructure. Information technology and service development are significantly influenced by cyber security. For the safety and economic well-being of the country, enhancing cyber security and preserving vital data infrastructures are very essential. The complete range of human endeavours, including business, banking, health care, energy, entertainment, communication, and national security, have come to rely on cyber networks. The breadth of the public's concern for privacy and personal information has grown, according to research results.

Rarely can we find a common method or reference model for security management in the current condition. The goal of this research project is to propose various kinds of algorithms or mechanisms that would allow people to engage effortlessly in the cyberspace without worrying about their safety. In order to do this, the present research has suggested numerous methods for resolving various security management concerns, such as reducing costs associated with cybercrime, credit card fraud, identity theft, cyber stalking, and phishing. This study is a modest

effort to comprehend the issue and provide some workable remedies. But there is a lot of room for study in the field of security management with reference to cybercrime.

REFERENCES

1) M. Rybnicek, R. Poisel, S. Tjoa, "Facebook Watchdog: A Research Agenda for Detecting Online Grooming and Bullying Activities", Proceeding in IEEE International Conference on Systems, Man, and Cybernetics, pp. 2854-2859, 2013.
2) R. Mordinyi, S. Biffl, "Versioning in Cyber physical Production System Engineering - Best-Practice and Research Agenda", Proceeding in IEEE/ACM 1st International Workshop on Software Engineering for Smart Cyber Physical Systems, pp. 44-47, 2015.
3) M. Savari, M. Montazerolzohour, Y. E. Thiam., "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application", Proceeding in International Conference of Cyber Security, Cyber Warfare and Digital Forensic, pp. 49-53, 2012.
4) Wu, G. Kaiser, "FARE: A framework for benchmarking reliability of cyber-physical systems", IEEE International conferences on Applications and Technology Conference (LISAT), pp. 1-6, 2013.
5) A. Stabek, P. Watters, R. Layton, "The Seven Scam Types: Mapping the Terrain of Cybercrime", Proceedings in 2010 Second Cybercrime and Trustworthy Computing Workshop, CTC '10, pp 41-51, IEEE Computer Society, 2010.
6) A. Rege, Z. Obradovic, N. Asadi, B. Singer, N. Masceri, "A Temporal Assessment of Cyber Intrusion Chains using Ultidisciplinary Frameworks and Methodologies", 2017 IEEE International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1-7, 2017.