IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

A Comprehensive Study on the Obstacles to the Internet Security in Recent Time

Gulista Khan, Associate Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- gulista.khan@gmail.com

ABSTRACT: ***Individuals often post a lot of personal information online, and some websites utilize this information for their own purposes as technology advances every day, making data security one of the most secure situations. Throughout this information analysis process, technical security is crucial. In recent years, data security has been put to the ultimate test. The first thing that springs to mind when discussing digital security is the "digital violations," which were multiplying quickly. Numerous strategies are being used by various organizations to counter these digital risks. Many individuals are nonetheless worried about digital security even with these protections. This paper primarily discusses the challenges that digital security confronts in light of recent technological advancements. Additionally, it places emphasis on the most recent statistics on trends, morality, and internet system security. Changing how computer security is conducted. The goal of this study's future work is to create and maintain excellent security at various levels.***

KEYWORDS: ***Computing, Cyber Security, Digital Security, Network, Security.***

1. INTRODUCTION

Cryptographic algorithms are the appropriate response. The Internet is now the foundation that has changed the most quickly in human history. Several ground-breaking inventions are altering the character of humanity in the current specialized environment. Due to the fact that we are unable to properly protect our personal information as a result of these developing technologies, the number of digital crimes is increasing at an alarming rate. This firm needs a high level of security since more than 60% of all financial transactions are now conducted online, enabling smooth and effective operations. Digital security has thus become a major topic in recent months. Data security in the IT business is simply one aspect of computer security; other areas, such as the network, are also covered. The benefits are identical to those of the administrative strategy. It is necessary to tackle digital misbehavior in a more complete and secure way. It is crucial that law enforcement authorities be given the resources they need to adequately investigate and punish digital misbehavior since expert estimates alone cannot stop all misconduct [1]–[3].

Several states and countries are increasingly establishing rigorous regulations on digital security to avoid the loss of important data. Everyone should be equipped with digital security to protect themselves from increasingly sophisticated online crimes. All technologies—aside from the most cutting-edge ones—need a high degree of security. Examples include parallel computing, compressed processing, electronic commerce, and internet banking. The security of these technologies has raised concerns since they deal with sensitive data. Must-have. For a nation's business and social development, it is essential to have cyber resilience and a solid data foundation. The development of new technologies depends on making the Network more secure (and safeguarding Internet users) [4]–[6].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

1.1.Cybercrime:

Any criminal behavior that uses a computer to do its crime and commit robbery is referred to as digital misbehavior. The US the Department of Justice has broadened the definition of "digital misbehavior" to include any illegal activity that requires a computer to provide evidence. The growing list of digital offenses, which are a serious problem for both individuals and nations, includes crimes made possible by computer systems, such as network disruptions and the spread of PC pathogens, as well as PC-based variations of existing crimes, such as data dishonesty, nagging, abusive language, and suspicion mistreatment. Digital misbehavior is often defined as misconduct carried out using a computer and the internet to steal someone's identity, sell stolen property, follow victims, or disturb routines via dangerous software. Digitaloffensess will increase in parallel with technical breakthroughs as technology continues to play an increasingly important part in everyday life. Worldwide civilizations continue to see sporadic spikes in cybercrime, notwithstanding a decline in traditional crime [7]–[9].

2. DISCUSSION

As long as there is evidence, a computer may be utilized (see digital forensics). The laptop may contain information in the form of a log file that investigators are interested in, even if it is not directly utilized for unlawful activities. Internet service providers are required by law to keep log files on file for a certain amount of time in the majority of nations. For instance, the Eastern Information Security Directive (which is applicable to all EU members) stipulates that all email traffic must be kept for at least a year.

Although many instances of cybercrime begin with an IP trace and may take many different forms, this is not necessarily a solid basis on which to build a case. Since many forms of widespread crime nowadays may include low-tech criminality, cybercrime investigators are a crucial part of law enforcement. Within the context of international cooperation, cybercrime investigative techniques are dynamic and constantly changing, whether they are used in open or closed police agencies.

2.1.Prevention:

In addition, the Department of Homeland Security created the Continuous Diagnostics and Mitigation (CDM) program. By identifying and prioritizing how to react to network dangers and instructing system staff accordingly, the CDM program analyses and safeguards government networks. By identifying risks early on, the Department of Homeland Security (DHS) has created Extended Cyber Security Services (ECS) to safeguard the American banking sector. Industrial Security Agency and InfoSec have acknowledged business partners that provide intrusion prevention services through ECS. An example of one of these services is DNS sink holing.

Law Cybercriminals target underdeveloped countries because their laws are easily exploited, allowing them to evade detection and punishment from law enforcement. In developing countries like the Philippines, there are few or no laws against cybercrime. Due to these loose constraints, hackers may launch covert attacks from across international borders. Even after being identified, these criminals avoid prosecution or deportation to a country like the United States which has passed laws that provide for punishment. While in certain circumstances this may be challenging, police enforcement agencies, For instance, The FBI has used trickery and deceit to catch criminals.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

For instance, the FBI has been trying to track down two Russian hackers for quite some time. Seattle, Washington-based counterfeit technology company was created by the FBI. The two Russians were then tempted. By offering them positions with this company, you may entice guys to travel to the United States. The suspects were captured once the questioning was finished outside the building. These cunning methods are often needed because lax legislation makes it difficult to apprehend cybercriminals in the absence of such regulation [10]–[13].

2.2.Penalties:

Penalties for computer-related violations might vary in New York State. There are several other punishments, ranging from a Class a misdemeanor like illegal computer usage to a Class C felony like first-level internet sabotage, which carries a sentence of 3 to 15 years in jail.On the other hand, some hackers have been hired by private corporations as information security professionals owing to their inside knowledge of computer crime, a practice that might cause market distortions. One suggested remedy is for courts to forbid convicted hackers from using the internet or laptops once they are freed from detention. However, given how pervasive computers have become in modern society, such punishments may be seen as excessive, harsh, and draconian. However, rather than outright banning the use of computers or the Internet, advanced methods for controlling cyber criminals' behavior have been developed. Under these processes, people are limited to using certain devices that are open to computer monitoring or processor searches by trial or bail authorities.

2.3.Awareness:

As technology advances, thieves try to steal more often, more people rely on the internet to update classified information like financial institutions or credit card numbers, and even more, people depend on the internet to update secret information like financial institutions or card numbers. More individuals use the internet to store secret material, including payment systems or credit card information, in order to maintain confidential information such as finance or card information fast-tracked. The danger posed by cybercrime to individuals worldwide is rising. It's becoming more and more important to raise awareness about how data collection is safeguarded and the methods thieves use to acquire it. In 2014, 269,422 complaints were submitted to the FBI's Internet Crime Complaint Center. It was calculated that the total claim loss would be $800,492,073. On the other hand, cybercrime seems to be on the minds of the common person. According to research, there are 1.5 million cyber-attacks every year, or about 4,000 per day, 170 per hour, or around three per minute, with just 16 percent of victims asking the attackers to stop. Knowing how to be safe while using the internet is essential since everyone who uses it might become a victim [14].

2.4.Intelligence:

An intricate ecosystem has developed to enable persons and businesses who wish to profit from cybercrime as its prevalence has grown. To mention a few, corporations that specialize in the sale of stolen goods, professional cybercrime firms, malware developers, and computer programmers have all been naturalized. These persons and organizations may be found thanks to the expertise, resources, and visibility of some of the most well-known cyber security firms in the world. These sources include a variety of protective knowledge, such as technical indicators like stolen file passwords or risky IP/URLs, as well as professional guidance on the objectives, tactics, and

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

operations of profiled groups. Information. While some data is accessible to the general public, the majority of users need a membership to a competing data provider in order to have continuing, regular access. Due to the infrastructure, tools, and threat intelligence of the threat actor, threat information is often addressed at the level of the single-cell threat actor, such as the actor's "TTP," or "strategy, technology, and practice." The other technological features are all distinct, and attackers may often easily change signs. Corporate industries are taking into account the significance of AI cyber security [15]–[17].

2.5.The Growth Of Cybercrime:

Investigation and prosecution of computer crimes are hampered by the global diffusion of cybercriminal activities. Since information on hacking groups has been freely published online, hackers have become less complex. Information sharing has tremendously benefited from blogs and groups; novices may now make use of the skills and direction of more seasoned hackers. Additionally, hacking is now more affordable than ever before: prior to the cloud computing era, spamming or scamming required a dedicated server, knowledge of Network operator standards, server management, network setup and management, and so on. On the other hand, today, hacking only requires a computer with an internet connection. A mail application is a mass, regular, low-cost, and easily spam Mable email sending service. Cloud computing might aid an activist in leveraging their assault by employing a one-time password, extending the scope of a botnet, or supporting a spamming operation.

Cyber security will always be at the center of every organization's safety procedures, according to knowledge. We are used to living in a world where all data is kept in an upgraded or digital format. When adopting human-to-human communication techniques, clients may feel secure when working with loved ones. In order to obtain personal information, cloud-based fraudsters will continue to target residential customers via popular social networking sites. In the framework of social infrastructure or during financial transactions, people must take all necessary safeguards. 98 percent of firms plan to retain or increase their digital security resources this year, with half of those resources going toward defending against online threats. As a result, a lot of businesses are getting ready for potential digital assaults [18]–[20].

There will be new attacks on Android-based devices, but they won't be that serious. In the not-too-distant future, reality tablets will be afflicted with a virus that affects certain PDAs since they utilize the same software. Mac ransom ware samples will continue to increase, but far more slowly than PC samples. Clients may create apps for almost any Windows XP 8-powered device (PCs, tablets, and high-tech mobile phones), enabling them to produce spyware similar to that seen on Android. Here are a few predicted patterns as a result of cleanliness in technology.

3. CONCLUSION

As the world becomes more connected and computers are utilized for everyday transactions, PC security has grown to be a significant issue. With every Modern Year that goes along, virtual malfeasance and data hygiene continue to deviate in novel ways. Businesses are being tested in terms of how they safeguard their infrastructure due to the most current and challenging advancements, as well as new digital tools and exposures that emerge on a regular basis. This also

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

necessitates new stages and expertise to do so. There is no one right way to address digital transgressions, but we should make every effort to do so in order to have a better and safer future on computers.

REFERENCES:

[1] R. Rondelez, "Governing cyber security through networks: An analysis of cyber security coordination in Belgium," *Int. J. Cyber Criminol.*, 2018, doi: 10.5281/zenodo.1467929.

[2] N. R. Sabar, X. Yi, and A. Song, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2801792.

[3] M. Kashif, S. A. Malik, M. T. Abdullah, M. Umair, and P. W. Khan, "A systematic review of cyber security and classification of attacks in networks," *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090629.

[4] Y. Raban and A. Hauptman, "Foresight of cyber security threat drivers and affecting technologies," *Foresight*, 2018, doi: 10.1108/FS-02-2018-0020.

[5] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*. 2018. doi: 10.1016/j.compind.2018.04.017.

[6] DfDCMS, "Cyber Security Breaches Survey 2018," *Cyber Secur. Breaches Surv. 2018*, 2018.

[7] UK Information Policy Team, "Aviation Cyber Security Strategy," *Open Gov. Licens.*, 2018.

[8] M. J. Cobb, "Plugging the skills gap: the vital role that women should play in cyber-security," *Comput. Fraud Secur.*, 2018, doi: 10.1016/S1361-3723(18)30004-6.

[9] R. Vignesh and K. Rohini, "Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security," *Int. J. Eng. Technol.*, 2018, doi: 10.14419/ijet.v7i3.27.17759.

[10] R. L. Brown *et al.*, "Lessons learned from our University Cyber Security Awareness Campaign," *J. Cybersecurity Educ.*, 2018.

[11] R. Setiawan, "Indonesia Cyber Security : Urgency To Establish Cyber Army In The Middle Of Global Terrorist Threat," *J. Islam. World Polit.*, 2018, doi: 10.18196/jiwp.2109.

[12] L. Hadlington, "Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," *Int. J. Cyber Criminol.*, 2018.

[13] G. Gluschke and M. H. Caşin, "Cyber Security Policies and Critical Infrastructure Protection," *Inst. Secur. Saf. Press*, 2018.

[14] B. Markelj and S. Zgaga, "Cyber security and cyber criminality of mobile device users in Slovenia," *Rev. za Kriminalistiko Kriminologijo*, 2018.

[15] J. Takahashi, "An overview of cyber security for connected vehicles," *IEICE Trans. Inf. Syst.*, 2018, doi: 10.1587/transinf.2017ICI0001.

[16] J. Collier, "Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision," *Polit. Gov.*, 2018, doi: 10.17645/pag.v6i2.1324.

[17] J. hua Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology and Electronic Engineering*. 2018. doi: 10.1631/FITEE.1800573.

[18] M. Ni, A. K. Srivastava, R. Bo, and J. Yan, "Design of A Game Theory Based Defense System for Power System Cyber Security," 2018. doi: 10.1109/CYBER.2017.8446449.

[19] T. Kelley, M. J. Amon, and B. I. Bertenthal, "Statistical models for predicting threat detection from human behavior," *Front. Psychol.*, 2018, doi: 10.3389/fpsyg.2018.00466.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

[20] T. T. Teoh, Y. Y. Nguwi, Y. Elovici, N. M. Cheung, and W. L. Ng, "Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data," 2018. doi: 10.1109/FSKD.2017.8393092.