AN EXAMINATION OF CYBER SECURITY DIFFICULTIES AND NEW TRENDS IN RECENT TECHNOLOGY

S. Shenbagavalli
Assistant Professor, Department of Electronics
G. Venkataswamy Naidu College (Autonomous), Kovilpatti

Received: December 05, 2023, **Accepted**: February 05, 2024, **Online Published**: February 15, 2024

ABSTRACT

Today, due to the modern lifestyle, people have joined technology life and are using more technology for shopping and financial transactions in cyberspace. At the same time, safeguarding of knowledge has become increasingly difficult. In addition, the heavy use and growth of social media, online crime, or cybercrime has increased. In the world of information technology, data security plays a significant role. Information security has become one of today's main challenges. Whenever we think of cyber security, we first think of 'cybercrimes,' which expand daily. Different governments and businesses take various steps to avoid this form of cybercrime. In addition to numerous cyber protection initiatives, many people worry about it. This paper focuses primarily on cyber security concerns related to the new technology. It also concentrates on the latest technologies for cyber security, ethics, and developments that impact cyber security.

Cyber security is essential in the realm of information technology since information security has emerged as one of the major concerns in the modern world. When discussing cyber security, the word “cyber-crimes,” which are on the rise, instantly comes to mind. Numerous governments and businesses are taking various actions to stop these cybercrimes. Despite these attempts, many individuals have severe concerns about cyber security. The main issue raised in this essay is how challenging it is to use cutting–edge technologies for cyber security. The most recent advancements in fashion, ethics, and cyber security.

Keywords: Cyber security, Cyber-crime, Cyberspace, cyber protection and Fashion

Introduction

Digitization in all aspects of human life, like healthcare, education, business, etc., has gradually led to storing all sorts of information, including sensitive data. Security is protecting digitized information from theft or physical damage while maintaining the confidentiality and availability of information. Still, as technology proliferates, the cybercrime rate is increasing in number and complexity. The reasons behind this tremendous growth in cybercrime are inadequate software, expired security tools, design flaws, programming errors, readily available online hacking tools, lack of awareness in public, high rates of financial returns, etc. Technical attackers develop more powerful attack tools to explore the vulnerabilities of the target and thereby attack the victim.

With this, new attacks in different variations are difficult to detect. The increase in internet dependency in all walks of life, the enormous amount of digital data accumulated through online transactions, and the decentralization of data repositories have led to the development of practical security algorithms. The continuously changing nature of cybercrime also leads to the difficulty of handling and avoiding emerging threats.

Securing cyberspace is the most challenging task, as advanced threats play a very active role. Therefore, it is necessary to get insights into security defense mechanisms, different techniques, and trending topics in information security. With the touch of a button, modern men can send and receive any data quickly, including email, audio, and video. But have they ever paused to consider how secure their data is in being carried to the recipient without compromise? Cybersecurity holds the solution.

The most quickly evolving contemporary technology is found on the internet. Modern Society is undergoing significant change as a result of numerous new technologies. Protecting our confidential info effectively is tricky because of these emerging innovations; cybercrime is rising.

Over 60% of secure network business dealings are now online, so this industry requires a secure network to verify the most trustable and transparent payments. Thus, the issue of cybersecurity is current. The scope of cyber security encompasses a variety of other domains, including cyberspace, in the IT segment, in addition to merely protecting data.

Recent technological innovations like cloud computing, mobile computing, online banking, and e-commerce require significant data. Since these technologies hold information about an individual, their security has become paramount. Any country's ability to maintain security and advance economically depends on preserving and enhancing its critical information infrastructure.

Cybercrime must be combated with ferocity and security. Since technological solutions cannot stop all crimes, it is critical to provide criminal control organizations with the necessary leeway to effectively investigate and prosecute cybercrime cases. Many nations and governments have enacted stringent cybersecurity laws to prevent acute data loss. All individuals must receive cyber security rules training to safeguard themselves from the increasing prevalence of cybercrimes. Everyone must get cyber security training to protect themselves from the growing wave of cybercrimes.

Literature Review

Julian Jang-Jaccard Improving cyber security and protecting critical information infrastructure is essential for each country's security and economic well-being. Safer Internet (watching Internet users) has been crucial to new services and the growth of public policy.

Lee, H.; Lee et al. Various attachment methods have emerged in the past, and the key logger is a representative attack tool that records all user's keyboard data entries and can be easily obtained from the Internet.

Mellado, D.; Mouratidis et al. Protection is an area in the SPL that has not been studied. Most methods concentrate on implementing safety criteria or properties in the SPL. There were various approaches to variability management and safety criteria from the early stages of product line production.

Mohsin, M.; Anwar et al., Whether the established techniques of feature models can be implemented or adapted for cyber security is the challenge in the field of cyber security. An approach is proposed to enhance the production and the derivative products of safe software product lines (SPLs). The techniques primarily used to achieve their goal. It sheds light on the overall structure of cyber-assault, its phases, and its impact on the financial system.

MdLiakat Ali, this study presents a brief overview of the cyber security problems raised by modern developments in technology and innovations; the paper also focuses on the latest cyber security strategies, trends, and ethics in cyber security.

Kutub Thakur Cyber security was used interchangeably for the security of knowledge, where it later saw the human's role in the safety process, although formerly finding this an additional dimension. However, such a debate on cyber safety has significant consequences since it reflects on the ethics of society as a whole. Various systems and models have been developed to solve the cyber security problem.

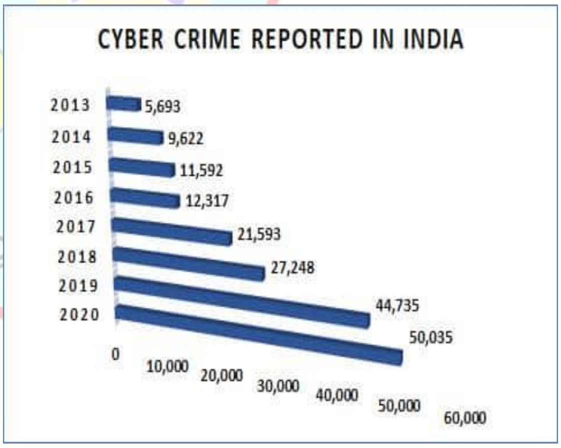
J. Li evaluated firewall issues and how the routing tables can be configured to minimize the firewall rule set, which helps avoid performance bottlenecks and limit safety breakthroughs. The problems are NP-full, and a heuristic approach has been suggested to demonstrate the efficacy of algorithms using simulations. Two significant contributions have also taken place.

Online crime

Any illicit activity that significantly relies on computers for both execution and theft is referred to as “cybercrime.” Currently, the U.S. Department of Justice classifies any criminal action that keeps computerized evidence as a type of cybercrime. The list of cybercrimes is constantly expanding and includes not only previously unheard-of-crimes that computers have made possible as network instructions and computer viruses spread but also computerized versions of crimes like identity theft, stalking, bullying, and terrorism, which have become significant problems for both individuals and countries. Cybercrime is a genetic term that describes any crime committed online, or cybercrime generally describes any crime committed.

Cyber Security

Data confidentiality is one of an organization's two most crucial safety measures. All information is now digitally or electronically saved due to the current state of our globe. Users can feel comfortable communicating with friends and family on social networking sites. The goal of cybercriminals will still be to steal personal information from residential users on social media sites. Individuals must take all necessary security precautions while working with banks and using social media.



CYBER SECURITY TRENDS CHANGING

Here is a summary of the trends that significantly affect cybersecurity

Website hosts

There is still a chance that web application security breaches will attempt to send malicious code or steal data. Cybercriminals spread their dangerous virus via legitimate web servers to which they have gained access. Data theft attacks are frequently reported in the media and present a severe risk. Data theft attacks are commonly reported in the press but present an extreme risk.

Data theft attacks are frequently reported in the media and present a severe risk. There is a greater need to prioritize the security of web servers and applications. Now, web servers and web applications need to be given more importance. Specifically, web servers provide the ideal platform for these cybercriminals to breach the system. It is essential to constantly use a secure browser to prevent falling victim to these scams, especially while carrying out basic transactions.

Service offered by cloud computing

Small, medium-sized, and large enterprises are steadily integrating cloud services. As a result, the earth is moving in the clouds' direction. This trend severely threatens cyber security because communications can evade established inspection locations. The policy restrictions for online apps and cloud services will need to be adjusted as the number of cloud-based applications increases to prevent the loss of essential data.

Security concerns are being raised even if cloud computing firms develop their protocols. While the cloud offers numerous benefits, it's important to remember that security risks are expanding along with the cloud.

APT's and specific Attacks

For long years, online filtering and instruction prevention systems (IPS)have been primarily dependent on Advanced President Thread (APT), an upgrade grade of cybercrime software, to detect such targeted attacks (often after the original contract). as attackers employ riskier and more sophisticated techniques, network security must interact with other security services to detect intrusions. Thus, we need to strengthen our security protocols to prevent introducing new threats.

Wireless Networks

These days, everyone on the earth can talk to everyone else. But these portable media must be safe. Firewalls and other security mechanisms grow more vulnerable as more people use tablets, phones, PCs, and other gadgets. This necessitates employing extra security measures on top of what the existing programs offer.

Always look for any security threats related to these mobile networks. Because mobile networks are more vulnerable to cybercrimes than other computer networks, extreme caution must be utilized in the event of any security difficulties.

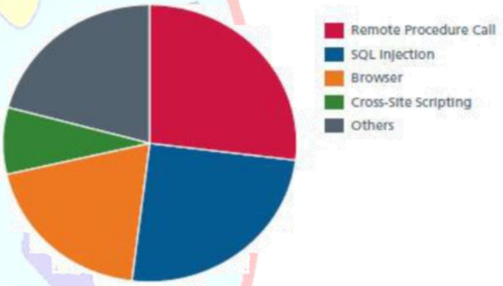
Internet Protocol Version 6

IPV6 is the newest iteration of the Internet Protocol (IP). It is designed to offer IP addressing and more security to support the predicted growth of linked devices in IOT, manufacturing, and new industries like autonomous driving. The more modern IPV6 system replaces the older IPv4 protocol, formerly functioning as the internet's building block. to protect IPV6, more than only IPv4 functionality must be migrated. Security policy must include some fundamental modifications to the protocol, even while IPv6 completely replaces IPv4 to expand the number of available private IP addresses.

Encryption of the Code

Data must be encrypted to prevent hackers and listeners from reading messages. The communications or information is encrypted using an encryption method to create an unintelligible cipher text. Identification often dictates how the message should be encoded throughout the encryption process. Encryption safeguards data integrity and secrecy at the most fundamental level. Furthermore, cyber security dangers spread across society as encryption is used more frequently. Mobile phones, wireless microphones, wireless intercoms, and data being carried over networks (like the Internet and e-commerce) are a few devices where encryption safeguards data in transit.

Therefore, the trends described above are some of those that are altering the worldwide cybersecurity scene.



Social Media Participation in Cybersecurity

Businesses must find creative ways to protect consumer information in a more socially and technologically linked world. Social networking will significantly enhance personal cyber threats and is essential for preserving cyber security. The usage of social media by employees is increasing, and so is the risk of assaults. Due to the widespread usage of social media and social networking sites by most people, these platforms have become vital resources for hackers seeking to obtain personal information and save critical data.

In a world where businesses can easily share personal data, they must be just as quick to recognize threats, act quickly, and prevent breaches. Due to their ease of use and ability to provide users with the information and data they need, these social media sites are utilized by hackers as bait. In addition to taking precautions to prevent information loss, users should use prudence when utilizing social media platforms.

One of the biggest challenges that media platforms present to businesses is the capacity for individuals to share information with a broad audience. Social networking also makes it possible for false information to propagate, which can be equally damaging. The Global Dangers 2022 report highlights the potential danger of quickly spreading incorrect information via social media.

These businesses can't give up on social networking sites since they are essential to their PR campaigns, even in the face of cybercrime risk. They need solutions that will make them aware of the threat so they can respond appropriately before any real damage is done. Businesses must be mindful of this to reduce risks, value information analysis, especially in social interactions, and implement the necessary security measures. Implementing precise policies and the appropriate technologies is needed to govern social media.

Advanced methods for cyber security

Security of passwords and access control

One of the most important things we've done to protect our data is to utilize a username and password. This could be a precursor to further cyber security protocols.

Verification of data

All credentials must be verified before downloading, necessitating that they come from a reliable and authentic source. The anti-virus software that was installed on the devices typically checks these papers. The devices also need top-notch antivirus software for virus prevention.

Malware scanner

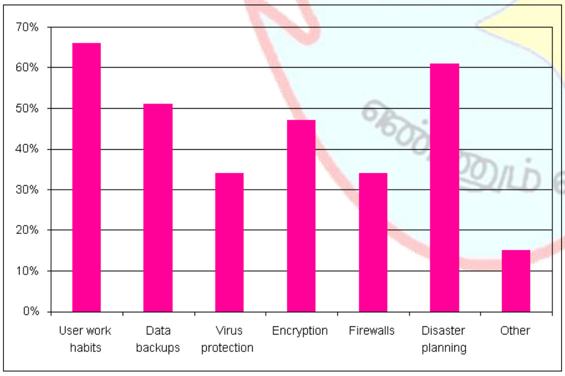
Usually, this program checks the computer's files and documents for malware and other harmful code. Malicious software, or malware as it is more commonly called, includes viruses, worms, and Trojan hordes.

Security devices

Hackers, worms, and viruses attempt to access your computer via the internet; however, a firewall is a hardware or software device that aids in thwarting this. Every message going into or coming out of the internet has to pass through the active firewall, which checks each one and stops those that don’t follow the predetermined security guidelines. For this reason, routers are necessary for malware detection.

Anti-virus software

An antivirus program is a computer program that hunts down hazardous malware, such as viruses and worms, and uses technology to reduce their impact. Most antivirus apps have an automated update capability that lets the program download virus profiles as soon as new ones are discovered, allowing it to start scanning for threats immediately. Antivirus software is an essential component of any device.



Ethics of The Internet

The principles of behaviour on the internet are referred to as online ethics. We have a fair probability of using the internet in a secure and morally responsible manner if we follow these cyber-ethics.

A handful of them are listed below:

- ➢ Do not be averse to online interaction and communication; it is simpler to stay in touch with friends and family, connect with co-workers, and exchange ideas and information with people locally or halfway across the world, thanks to electronic mail and texting.
- ➢ Stay away from online bullying. Avoid making fun of others, spreading false information about them, sending embarrassing images, and engaging in any other behavior that can endanger them.
- ➢ Since the internet is considered the most extensive library in the world and has knowledge on almost any topic, it is crucial to utilize it responsibly and legally.
- ➢ Never access another person’s account using their password.
- ➢ You should never try to infect someone else’s computer with malware, and you should never give out any personal information to anyone because you never know how someone else might turn it against you.

- Always be authentic when interacting with others online, and avoid making up false accounts of other people since this could land you both in hot water.
- Always be aware of content protected by copyright, and only download games and videos that are allowed.

These are some guidelines for online behaviour that one should follow. We learn the correct behaviours from a young age, which is true online.

Conclusion

The use of networks for essential business activities and the growing global interconnectedness have elevated the significance of computer security. Cybercrime is a rapidly evolving area, and information security is no different. Regarding the methods employed to defend facilities and the required opportunities and abilities, organizations must deal with the most recent and cutting-edge technology and the new cyber tools and dangers that arise daily. Future virtual environments must be trustworthy. Thus, we must do everything in our power to combat cybercrime. There isn’t a perfect response, though.

The enormous increase in Internet access and the progress of Internet-enabled devices, the rising numbers of the population, and widespread Internet use frequently show susceptible personal data with little realization of the implications of information leakage.

- We speculate that concerns relating to end-user confidentiality will rise in line with the increasing amount of knowledge accessible on the internet in the future.
- Furthermore, usability issues are becoming increasingly relevant as a way of intuitively learning about and using end-user-oriented protection mechanisms without complicating
- or profound learning curves to secure the data. Cyber safety practice in the community is built up with innovative patches that rectify existing security and confidentiality problems and move on them.
- Some believe this revolutionary strategy has failed and will be unable to fulfill future requirements because the original Internet was invented in a somewhat different context from how it is used today. An approach to "thinking beyond" is suggested to better use the increasing demands of the future without referring to the existing computing system and future, but to start again.

References

Belapure, S., & Godbole, N. (n.d.). Cyber Security: Understanding Cyber Crimes.

Corrons, L. (2012). A Look Back on Cyber Security 2012. Panda Labs.

Krause, A. (n.d.). Computer Security Practices in Non-Profit Organisations – A NetAction Report.

Kumar, A. (2013, September 3). Cyber security in Malaysia. CIO Asia, H1 2013.

Li, J. (2015). The research and application of multi-firewall technology in enterprise network security. International Journal of Security and Its Applications, 9(5), 153–162.

Lyne, J. (n.d.). Eight trends are changing network security. Sophos Article 04.12v1.DNA.

Reddy, G. N., & Reddy, G. J. U. (2013). Study of Cloud Computing in the Healthcare Industry. International Journal of Scientific & Engineering Research, 4(9), 68–71. https://www.ijser.org

Thakur, M. A., Atobatele, B., Thakur, K., Qiu, M., Gai, K., & Ali, M. (2019, July 8). Challenges of Cyber Security and the Emerging Trends. BSCI'19. Auckland, New Zealand.

Thakur, K., Qiu, M., Gai, K., & Ali, M. (2015). An Investigation on Cyber Security Threats and Security Models. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing. https://doi.org/10.1109/CSCloud.2015.85