COMPUTER NETWORK SECURITY AND PREVENTION STRATEGY ANALYSIS

[1]Swaroop p.r,[2]Alwin k varkey,[3]Akhila k.h

[1] BCA Student, [2] BCA Student, [3]Assistant Professor
Department of Computer Application
SNGIST ARTS AND SCIENCE college,
Manakkapady Karumalloor (P.O) North Paravur, Ernakulam Kerala, India - 683511

Abstract: The standard of living today is far better than it was in the past. Computers, in particular, have significantly impacted how convenient people's lives are. As aspirant young adults in the modern world, we should be conscious of the conceivable risks connected with the computer networks while simultaneously enjoying its ease. We might not be very aware of the conceivable hazards associated with computers in our daily lives. This is due to the circumstance that, at the instant, we only utilize computers in relatively limited spaces like families, workshops, campuses, etc. There is a robust probability that a variety of problems will arise if we use computers widely. This paper targets a way for successfully perform network protection technology and are searching for systematic anticipation strategies, hopeful to offer robust guide for internet safety.

Keywords: - Network Security, Safety Technology, Preventive Strategies, Analysis and Discussion.

1. INTRODUCTION

Computer network technology has advanced substantially over the past few decades and achieved major development outcomes. People may now effortlessly gather data via smart phones anytime, anywhere, eliminating the constraints of time and place as well as reducing the barrier among individuals, just as they could with the "big head computer" in the beginning. Yet, there are also significant security threats that are concealed even under flawless scientific and technological advancements. The accessibility and social equality of Internet technology serves as a pointy end for thieves to breach individuals' private asset as it becomes incorporated into every area of people's lives. Every citizen's freedom and desires are impacted by the safety of network systems. The core and basis of how we can accomplish the network's promising future development is enhancing network security technologies and developing successful preventive techniques.

2. COMPUTER NETWORK SECURITY VULNERABILITY TRAITS

2.1 THE DIFFUSIVITY IS STRONGER AND THE ABRUPTNESS IS LARGER

As most of us are aware, a computer network is generated in a digital world. When the vulnerabilities of network-type information manifest, it is more appropriate to hide it, making it problematic to locate and, thus, challenging to influence in an operative manner. When a security weakness strikes a computer network, it can spread entirely in a moment. But still, most of the time, because of unanticipated factors and extreme camouflage, users are unable to search for operative solutions in time to control and fix them. This feature is also being used by the community security vulnerability to widen the breadth of its effects, which has an unanticipated effect on the state of the network's overall security, people's daily lives, and even influence society's overall safety regulations.

2.2 THE CONCEALMENT IS HIGHER AND THE LATENCY IS GREATER

Computer viruses of all kinds share a great deal in common with security weaknesses in the computer community. It might spend long time hiding in the web's crevices, but as soon as the network atmosphere seems to have "POOR IMMUNITY" or a Longstanding virus accumulation, there could be a instant when computer community safety is compromised. Some computer systems lack the necessary virus removal security software, which provides an excellent living environment for the infection to survive. As a result, the virus rapidly spreads to every point of the computer network by constantly splitting and replicating. In the end, the entire computer network is harmed, resulting in significant losses and problems for the users.

3. THE STATE OF COMPUTER NETWORK SECURITY

3.1 COMPUTER NETWORKS' SECURITY IS JEOPARDISED BY VIRUSES.

Underneath regular situations, the most common source of computer network disruption is virus propagation. Whenever a network is invaded by a ransomware virus, for example, the virus can duplicate it's own endlessly in a relatively short time period, concentrated on the whole computer system. It is also capable of operating in a very brief duration, with the network of information as well as network speed and different way to unfold, throughout this method of setting a connection which could robotically join different network nodes, and for its strategy to assault, eventually leading towards the entire computer network paralysis. This sort of viral vulnerability hassle is the prevalence of excessive possibility throughout people's each day existence, the occurrence of especially not unusual damaging phenomenon. This necessitates the creation of a sensible and environmentally friendly method of

computer network virus attack, which will reduce the prevalence of malware issues on the computer network intrusion harm such a concept, in order to ensure that individuals can use network functionally and effortlessly.

3.2 COMPUTER NETWORK LEAKAGE AS A RESULT OF INAPPROPRIATE USAGE

The structure of a computer network isn't always straightforward because it's built from cutting-edge technological know-how and generation, and its own sturdy complexity, and the security software associated with the pc. Most computer users lack a competent execution level, so when implementing a virus protection software, the users are unable to differentiate the method of software specification and the hardware requirements of the computer, to select the appropriate security software. In this instance, it results many users in the usage of computer networking or network security software installation method, there isn't a cost-effective and practical operational conduct. There are some users who are unaware of any concealed security issues in the store network during the method of using the computer network. It is difficult to ensure the safety of the network when using the network, which may result in much less use of the computer and even a considerable decrease in the network safety index. Most users wish to fix vulnerabilities in the network, but due to a variety of reasons, there can be difficulties in restoration. The total restoration requires a significant amount of effort and time. As a result to this issue, a variety of network structures have entered the market. A few of them fail to pass legal certificate or they simply purloin the resources of qualified software development teams to create unlicensed systems , these software didn't efficiently give a boost to network safety, but due to the misuse of these software are now more vulnerable to some network security issues, or even result in extortion.

3.3 HACKER ASSAULTS ON NETWORKS

One of the various security issues that could cause computer networks to collapse is undoubtedly the attack from hackers, which threatens the continued functioning of public data in grave danger. By identifying a network vulnerability, these hackers can take private or priceless information from a target computer. They have the ability to gain unrestricted access to the internet, trespass on, or maliciously take private information or assets from the targeted device. Currently, the globe is in an Internet growth phase where nations and individuals have realized social connectedness. In this setting, the Online world had undergone fully interconnected growth with the highest levels of inclusivity and transparency. If a skilled hacker chooses to assault a specific network, this could result in significant losses for the entire network, hence it needs to be noticeable.

3.4 THE USAGE OF COMPUTER SOFTWARE PROGRAM

If you want to use the communications system further productive and for a long time, you must be able to guarantee protection of computer code. Because the computer network is a digital and powerful machine development within the process of system and software compilation. There will inevitably be an increase in the number of security flaws. When a network device is ready for use, if the user operates it incorrectly or uses it incorrectly, security flaws will inevitably occur. It is still common for cybercriminals to arrange things unlawfully by trying to take advantage of a hedge limiting factor overwhelm in computer software. According to prior experience, the community environment will be fairly unstable if the relevant body of workers fails to record effective corrective measures into the computer network at some point throughout the education of software program and device. To the greatest extent possible, this issue needs to be taken into account in the design of the structure to minimize any potential dangers to community safety.

4. STRATEGIES TO ASSURE THE SAFETY OF COMPUTER NETWORKS

4.1 EMPLOY DATA ENCRYPTION TECHNIQUES

The crucial generation of data encryption must not be separated from the computer network for it to function correctly. Record encryption has a significant impact on community operation. It has the potential to effectively safeguard the security of personal information and identity data. As a result, it may also employ coding and encryption technology to conceal private data and individual records more thoroughly. Encryption is more effective than other network security measures because it is more resistant to unknown attacks and unauthorized entry, which could prevent cybercriminals or viruses from gaining sensitive information more easily. The nicest software of this innovation, for the most part, can successfully fend off peer record theft by illegal organizations. Data encryption technology can actually boost the probability of computer networks running securely, allowing for the transmission and storage of more comprehensive and comfortable data. Furthermore, unique record encryption techniques have their own unique qualities that provide solid assurance for the community's operation.

4.2 ESTABLISHING FIREWALL MECHANISM

I believe that the use of the phrase "firewall" is not odd. This technology isn't just extensively used in computer systems; it also has a significant impact on how smart phones are protected. Firewall, which is also an important technology in the community security, can support the greatest improvement of the business potential of the network when it is set up within the community records control. The fundamental idea behind the use of firewall technology is to establish an excellent exterior isolation system within the neighborhood. It creates centered network access privileges in accordance with the actual desires, especially for the channels of the outside community and the user firms of the outside community that could successfully limit the hostile entry of the public networks to the corporate network, to effectively minimize the opportunity that thieves need to obtain private information unfairly. avert potential customer losses. Not only can firewall technology facilitate secure data transfer across networked computers, but it can also precisely and thoroughly demonstrate how the entire network is operating. When a problem arises in the community for the first time, the research problem can be quickly secured and reported to the appropriate personnel, and a secure operating environment for the computer network is created.

4.3 TECHNOLOGY FOR VULNERABILITY SCANNING

The term "security scanning generation" describes a generation that may accidentally discover and check the computer's security status at every moment when using the computer network. It can accurately identify any potential underlying issues with the laptop. When users encounter security risks during the aid collection methods, security scanning will nearly terror to aid manipulators become aware of the safety of records. Such technique may be very all-encompassing, using the existing network as the machine's field of view for detection while scrupulously looking for problems that could possibly exist in the network. In a similar manner, it may track community susceptibilities in actual time throughout routine usage. When the issue is identified, it will reply instantly. Technology for security scanning is too essential to achieving lengthy safety improvements for computer networks.

5. SAFETY MEASURES FOR MANAGING COMPUTER NETWORKS

5.1 BOLSTER COMPUTER NETWORK SYSTEM MANAGEMENT

Consider the strategy of the network safety access permission as the basic assurance, then consider the individual access period as the step forward, if you need to create a fantastic community records administration system then increase the network's safety. Clinical and cost-effective management of authorization periods, building on this to support the established hierarchy of server safety features, and continuing to optimize and enhance the networking administration system.

Similar to this, it ought to be able to independently and privately lower back up all user data, which is a good way to increase user engagement when issues arise. The machine required for backup will also be capable of ensuring its proper development and forethought, capable of continuously updating its own machine while being used, so that it can effectively fulfil its function.

5.2 SET UP A NETWORK SECURITY UPKEEP GROUP

The introduction of the fresh age of computer network data safety cannot be an concession, as any business and sport are inextricably bound by the restrictions of the tool and regulation. In order to protect the core interests of the masses, the systems development division must be able to create practical countermeasures that are both affordable and effective. These countermeasures must effectively prevent intrusion from outside the community and minimize any user shortage. At that time, the appropriate divisions must commence by enhancing the computer network device's security control system. Build a team with the right expert perspective and extensive hands-on involvement, screen the computer network in actual time, and have the aptitude and usefulness to discover solutions to issues when issues and concealed risks are located. After issues, concealed risks are identified, we must be capable to quickly and effectively identify solutions. To persist with the times and network while continuously raising both their level, group members must be capable to perform daily drill of network directors' applicable technical expertness and procedure ideals in the manner of labor. The necessary sections must assign responsibilities to each person, clearly outline the extent of each person's personal responsibility, and rigorously implement network protection control duties in order to protect the computerized program's activities and those of all users.

5.3 VIRUS PREVENTION AND CONTROL

The security of network data is at risk as a result of all types of malware pattern evolving along with the growth of the laptop community. As defense mechanisms progress, existing virus means are very complex, sophisticated, and self-restoration. In order to handle this example, we must first be able to perform an excellent process within the category of virus types that is organised and ready to categories the actual state of the virus and the actual condition of the laptop system. For specific types of viruses, users should be able to create suitable security apps. When developing the security software, we must be careful to incorporate tools could successfully block a heterogeneity of virus. After a user decides to examine a computer network for viruses, It's also crucial to touch twice the appropriate anti-malware application to perform thorough and multidirectional recognition and checking, allowing for the early detection and elimination of the malware.

6. MAJOR FINDINGS

- Encryption is more effective than other network security measures because it is more resistant to unknown attacks and unauthorized entry.
- Firewall mechanism isn't just extensively used in computer systems.It also has a significant impact on how smart phones are protected.
- Vulnerability scanning will discover and check the computer's security status at every moment when using the computer network.
- Computer network system management is a good way to increase user engagement when issues arise. In order to protect the core interests of the masses, the systems development division must be able to create practical countermeasures that are both affordable and effective.
- The user need to use appropriate anti-malware application to perform thorough and multidirectional recognition and checking, allowing for the early detection and elimination of the malware.

7. CONCLUSION

Computer networks are currently assisting social science and technology to innovate and make breakthroughs, and they have become an essential component of people's daily lives. We must be able to significantly increase our understanding of computer network security concerns in order to identify effective ways to reinforce security and security protection measures. Also, pertinent state departments should be able to create and enhance pertinent rules and protocols aimed at this issue, increase the oversight of network safety, and create opportunities for a practical, effective, and dependable growth of computer networks. The discussed strategies offer several benefits, including protection of confidential information such as financial and personal information, mitigation of cyber-attacks achieved by implementing network security prevention strategies that can minimize their occurrence, compliance with regulatory standards, increased productivity by enabling work without worrying about cyber threats, and reduction of downtime by ensuring that systems are up and running at all times.

8. ACKNOWLEDGMENT

We are very thankful to the entire researchers who have done the excellent for drawing attention to the computer network security and prevention strategies.

REFERENCE

1. Sklavos Nicolas, Kaaniche Nesrine On the design of secure primitives for real world applications [J] Microprocessors and Microsystems, 2021, 80.
2. Rathee Geetanjali, Ahmad Farhan, Sandhu Rajinder et al. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things [J] Information Processing and Management, 2021, 58(3).
3. Rajeesh Kumar N.V., Mohan Kumar P. Application of SDN for secure communication in IoT environment [J] Computer Communications, 2020, 151(c).