Cybersecurity Types and Prevention Methods

Anush Sharma,
Assistant Professor, Dept of CSE
Sujal Nangla, Anadya Kaushal, Neha Soel,
Student, Dept of CSE
HIET, Kangra, HP, India

ABSTRACT

As the technology is still developing, we have several of technologies which are helpful to humans but at the same time they contain many limitations. One of the such technology in the today's modern world contains every information to be stored in databases of computers and there are several chances of attacks on their data which is known as **cybercrime**, to stop such digital crimes there is introduced a shield known as cyber security. In every field whether military, corporate organization, intellectual property, stock market, banks etc.

"This abstract explores the fundamental concepts of cyber security; it's challenges and the strategies employed to migrate risks and protect the digital world."

Keywords: Cybercrime, Digital crime, Cyber security, Cloud computing.

INTRODUCTION

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It's used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems and smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From digital banking to digital marketing, email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information security.

The term "cybersecurity" applies in a variety of contexts, from business to mobile computing, can be divided into few common categories as ….

NETWORK SECURITY: is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malwares and Etc.

APPLICATION SECURITY: It involve protecting software and devices from unwanted threats and malwares. The application security defends unauthorized access and connected servers. Despite the best efforts to prevent unauthorized access there are still lot of chances that threats can occur.

CLOUD SECURITY: It protects cloud-based assets, services and infrastructure. It is a shared responsibility model. Cloud service providers handle the access to the authorized users.

ENDPOINT SECURITY: Endpoints such as mobile devices, desktop, servers etc. are the most usual points for digital threats. Thus, the endpoint security prevents from the cyber-attacks which is the most common point for digital threats.

MOBILE SECURITY**: It protects the mobile devices from the digital threats. The threats can be prevented on such devices as tablets, phones and laptops etc. from mobile security.**

The spectrum of cyber-attacks: has broadened significantly, driven by advancements in technology. Common threats include Distributed Denial of Service (DDoS) attacks, phishing schemes, and malware infections. Traditional protection systems are proving inadequate against these new-generation attacks, necessitating innovative solutions that leverage machine learning and deep learning techniques for detection and prevention (Aslan et al., 2023).

Emerging technologies such as cloud computing, the Internet of Things (IoT), social media, and cryptocurrencies have contributed to the complexity of the cyber threat landscape. These technologies not only provide new opportunities for innovation but also introduce unique vulnerabilities that cyber criminals exploit (Aslan et al., 2023).

Insider Threats

Insider threats represent a significant challenge in cyber security. Gheyas and Abdallah (2016) conducted a systematic literature review and meta-analysis on the detection and prediction of insider threats, revealing various methodologies and frameworks that can be employed to mitigate these risks. This highlights a critical area where organizations must focus their efforts, as insider threats often bypass traditional perimeter defenses.

Vulnerabilities in Emerging Technologies

Internet of Things (IoT)

The IoT environment faces numerous vulnerabilities due to the integration of various devices and data streams. Tsiknas et al. (2021) identified major vulnerabilities specific to Industrial IoT (IIoT) systems and proposed multilevel security approaches to counter these risks. The interconnected nature of IoT devices necessitates comprehensive security measures that consider both device-level and network-level vulnerabilities.

Cloud Computing

Cyber security threats in cloud environments are also a pressing concern. Nafea and Almaiah (2021) reviewed common threats faced by cloud systems, emphasizing the need for research on security and privacy challenges in big data environments. As organizations increasingly migrate to the cloud, developing robust security frameworks that address these challenges is paramount.

Maritime and Drone Security

Recent studies have extended the discussion of cyber threats to specific industries. Farah et al. (2022) highlighted vulnerabilities in the maritime sector, particularly concerning the Global Navigation Satellite System (GNSS).

Similarly, Majeed et al. (2021) proposed a framework for enhancing security in IoT-aided drones, utilizing machine learning models to bolster privacy measures. These findings underscore the necessity for industry-specific approaches to cyber security.

Privacy Risks and Ethical Considerations

The collection of vast amounts of data by cyber security systems poses significant privacy risks. Toch et al. (2018) proposed a taxonomy for assessing privacy risks in information security technologies, focusing on aspects such as data exposure, user identification, data sensitivity, and user control. This highlights a crucial area where cyber security professionals must balance the need for security with the imperative to protect user privacy.

Innovations in Cyber Security Solutions

Machine Learning and Deep Learning Approaches

Innovative approaches employing machine learning and deep learning are gaining traction in the cyber security domain. The SHADEWATCHER system utilizes data provenance analysis and graph neural networks to enhance cyber threat detection, addressing limitations in existing methodologies by reducing false alarms and improving detection effectiveness (Zengy et al., 2022). Moreover, Tayyab et al. (2022) emphasized the need for efficient feature extraction and analysis in deep learning-based malware detection. These advancements reflect a shift toward more sophisticated and adaptive cyber security solutions.

Explainable Artificial Intelligence (XAI)

The demand for transparency and explain ability in machine learning models is growing, especially in cyber security. Kuppa and Le-Khac (2020) proposed a taxonomy for Explainable Artificial Intelligence (XAI) methods relevant to security properties and threat models. This focus on explain ability is essential for building trust in automated systems, particularly in scenarios where decisions made by AI have significant consequences.

Financial Implications of Cyber Crime

The financial impact of cybercrime is substantial. Sharif and Mohammed (2022) presented data on the increasing costs associated with cyber prevention and management, highlighting trends in cybercrime statistics. Understanding these financial implications is critical for organizations as they allocate resources toward cyber security measures.

Challenges in Digital Forensics

Digital forensics presents unique challenges in the context of cyber security. Sharma et al. (2019) emphasized the need for advancements in various forensic domains to address challenges related to cyber threats and malware. As cyber attacks become more sophisticated, the field of digital forensics must evolve to keep pace with emerging threats.

Knowledge Gaps and Future Research Directions

Despite the extensive research on cyber security, several knowledge gaps persist. For instance, while many studies focus on specific types of attacks or sectors, there is a need for comprehensive frameworks that integrate findings across different domains. Additionally, the ethical implications of data collection in cyber security systems warrant further exploration, particularly in light of increasing regulatory scrutiny.

Future research should also prioritize the development of adaptive cyber security solutions that can respond to the dynamic nature of cyber threats. The integration of emerging technologies, such as blockchain and quantum computing, into cyber security frameworks may offer new avenues for enhancing security and resilience.

Conclusion

The literature on cyber security and its threats is expansive and continually evolving. As technology advances, so do the tactics employed by cyber criminals. This review has synthesized key findings in the field, highlighting the multifaceted nature of cyber threats and the innovative approaches being developed to combat them. By addressing the identified knowledge gaps and exploring future research directions, the cyber security community can better prepare for the challenges that lie ahead.

Graphs and Recent Data

Graph 1: Trends in Cyber Crime Statistics Over Time

``````

These graphs illustrate the upward trend in cyber crime incidents and financial losses, as well as the distribution of different types of cyber attacks in recent years.

In conclusion, as the digital landscape continues to evolve, so too must our understanding and approach to cyber security. Continued research, collaboration, and innovation are essential to safeguarding against the ever-growing array of cyber threats.

## References:

1. Tayyab, Umm-e-Hani., Khan, Faiza Babar., Durad, M. H.., Khan, Asifullah., & Lee, Yeon Soo. (2022). A Survey of the Recent Trends in Deep Learning Based Malware Detection. <i>J. Cybersecur. Priv.</i> , 2 , 800-829 . http://doi.org/10.3390/jcp2040041
2. Kuppa, Aditya., & Le-Khac, Nhien-An. (2020). Black Box Attacks on Explainable Artificial Intelligence(XAI) methods in Cyber Security. <i>2020 International Joint Conference on Neural Networks (IJCNN)</i> , 1-8 . http://doi.org/10.1109/IJCNN48605.2020.9206780
3. Aslan, Ömer., Aktuğ, Semih Serkant., Ozkan-Okay, M.., Yilmaz, Abdullah Asim., & Akin, Erdal. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. <i>Electronics</i> . http://doi.org/10.3390/electronics12061333
4. Tsiknas, Konstantinos G.., Taketzis, Dimitrios., Demertzis, Konstantinos., & Skianis, C.. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. <i>IoT</i> . http://doi.org/10.3390/IOT2010009
5. Nafea, Roaa Al., & Almaiah, Mohammed Amin. (2021). Cyber Security Threats in Cloud: Literature Review. <i>2021 International Conference on Information Technology (ICIT)</i> , 779-786 . http://doi.org/10.1109/ICIT52682.2021.9491638
6. Majeed, Rizwan., Abdullah, Nurul Azma., Mushtaq, Muhammad Faheem., Umer, Muhammad., & Nappi, M.. (2021). Intelligent Cyber-Security System for IoT-Aided Drones Using Voting Classifier. <i>Electronics</i> . http://doi.org/10.3390/electronics10232926
``````

7. Vinayakumar, R.., Soman, K.., Poornachandran, P.., Mohan, Vysakh S.., & Kumar, Amara Dinesh. (2019). ScaleNet: Scalable and Hybrid Frameworkfor Cyber Threat Situational AwarenessBased on DNS, URL, and Email Data Analysis. <i>J. Cyber Secur. Mobil.</i> , 8 , 189-240 . http://doi.org/10.13052/JCSM2245-1439.823
8. Joseph, D.., & Norman, J.. (2019). An Analysis of Digital Forensics in Cyber Security. , 701-708 . http://doi.org/10.1007/978-981-13-1580-067
9. Teichmann, F.., Boticiu, Sonia R.., & Sergi, B.. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?. <i>International Cybersecurity Law Review</i> , 4 , 259 - 280 . http://doi.org/10.1365/s43439-023-00095-w
10. Zengy, Jun., Wang, Xiang., Liu, Jiahao., Chen, Yinfang., Liang, Zhenkai., Chua, Tat-Seng., & Chua, Zheng Leong. (2022). SHADEWATCHER: Recommendation-guided Cyber Threat Analysis using System Audit Records. <i>2022 IEEE Symposium on Security and Privacy (SP)</i> , 489-506 . http://doi.org/10.1109/sp46214.2022.9833669
11. Vinayakumar, R.., Soman, K.., Poornachandran, P.., Akarsh, S.., & Elhoseny, M.. (2019). Deep Learning Framework for Cyber Threat Situational Awareness Based on Email and URL Data Analysis. <i>Advanced Sciences and Technologies for Security Applications</i> . http://doi.org/10.1007/978-3-030-16837-76
12. Makawana, Pooja R.., & Jhaveri, Rutvij H.. (2018). A Bibliometric Analysis of Recent Research on Machine Learning for Cyber Security. , 213-226 . http://doi.org/10.1007/978-981-10-5523-2_20
13. Sharif, Md Haris Uddin., & Mohammed, Mehmood Ali. (2022). A literature review of financial losses statistics for cyber security and future trend. <i>World Journal of Advanced Research and Reviews</i> . http://doi.org/10.30574/wjarr.2022.15.1.0573
14. Rachit, ., Bhatt, Shobha., & Ragiri, Prakash Rao. (2021). Security trends in Internet of Things: a survey. <i>SN Applied Sciences</i> , 3 . http://doi.org/10.1007/s42452-021-04156-9
15. Farah, Mohamed Amine Ben., Ukwandu, Elochukwu A.., Hindy, Hanan., Brosset, David., Bures, Miroslav., Andonovic, I.., & Bellekens, X.. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. <i>Inf.</i> , 13 , 22 . http://doi.org/10.3390/info13010022
16. Amini, Amir., Ghafouri, Mohsen., Mohammadi, Arash., Hou, Ming., Asif, A.., & Plataniotis, K.. (2022). Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation Under Cyber Attacks. <i>IEEE Transactions on Smart Grid</i> , 13 , 3188-3202 . http://doi.org/10.1109/TSG.2022.3159582
17. Sharma, B.., Joseph, Michelle Ann., Jacob, Biju., & Miranda, Lt. Col. Bryan. (2019). Emerging trends in Digital Forensic and Cyber security- An Overview. <i>2019 Sixth HCT Information Technology Trends (ITT)</i> , 309-313 . http://doi.org/10.1109/ITT48889.2019.9075101
18. Toch, Eran., Bettini, C.., Shmueli, E.., Radaelli, Laura., Lanzi, A.., Riboni, Daniele., & Lepri, B.. (2018). The Privacy Implications of Cyber Security Systems. <i>ACM Computing Surveys (CSUR)</i> , 51 , 1 - 27 . http://doi.org/10.1145/3172869
19. Gheyas, I.., & Abdallah, A.. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. <i>Big Data Analytics</i> , 1 , 1-29 . http://doi.org/10.1186/S41044-016-0006-0
20. Chakraborty, Chinmay., Nagarajan, Senthil Murugan., Devarajan, Ganesh Gopal., Ramana, T. V.., & Mohanty, R.. (2023). Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method. <i>ACM Transactions on Sensor Networks</i> . http://doi.org/10.1145/3597210