Emerging Threats and Innovations in Cybersecurity

DEEKSHA SONAL[1], SANSKAR[2], KUNAL[3] HIMANSHU RAWAT[4]
[1,2,3,4] *Department of Computer Science and Engineering, Chandigarh University Mohali, Punjab, India*

Abstract- ***As the technology is evolving, new smart devices are being introduced. this opens up an opportunity for attackers to launch their devices as along with technology, attacking techniques are also evolving. The concept of cybersecurity is not new as it dates back to 1960s. Although the type of attacks have changed and even defense mechanism towards said threats are also evolving, still there remains a gap between attacker's methods and the technologies available to tackle them. Interconnectedness of multiple devices via IOT(Internet of things) has turned up to be a major opportunity for attackers to launch new attacks namely man-in-middle attack, DOS(denial of service) etc. Social engineering still remains as a major threat in terms of data theft and fraud. In this paper, various attack techniques are studied along with the methods used to prevent and eradicate threats posed by attackers. It also focuses on the fact that human error is the cause of majority of cyber incidents. The analysis on human error focuses on finding ways to minimize such errors. A significant portion of review focuses on how outdated cybersecurity techniques are still being used in multiple institutions and showcases the advantage new methods have in tackling threats and attacks efficiently. This study also showcases latest trends in field of cybersecurity and emerging threats. It also discusses the working of various tools used in the field of cybersecurity and their effectiveness for example- firewalls, anti-fraud systems.***

Index Terms- ***Cybersecurity, Threats, Theft, Fraud, Authentication, Authorization, Social-Engineering***

I. INTRODUCTION

Internet has revolutionized the way of data sharing and communication. This revolution certainly has increased the efficiency of our systems and made our lives easier. But rapid growth of new technologies has also resulted in new cybersecurity risks and weaknesses, calling for a rigorous examination of these issues. The earliest case of cybersecurity threat was the Creeper Virus which was detected in 1970's. Although it started as an experiment and it did not steal or manipulate any data but it clearly depicted the need of strong cyber security mechanisms.

Cybersecurity attacks have grown dramatically over time, becoming increasingly sophisticated and dangerous. In the early days of computing, threats were primarily limited to basic viruses and worms intended for pranks or minor interruptions. However, as technology advanced and the internet became more prevalent, cyber threats evolved into highly organized and targeted attacks.

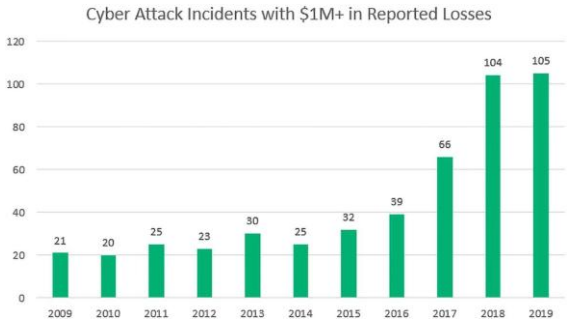
Ransomware, phishing, and nation-state-sponsored cyber warfare are all examples of modern cybersecurity dangers. Hackers are now using AI and automation to launch large-scale attacks. The growth of the Internet of Things (IoT) and cloud computing has extended the attack surface, making cybersecurity an ongoing concern. To keep up with hackers, firms must implement proactive security measures such as threat intelligence, machine learning-based protections, and powerful encryption.

The traditional attacks include: -

1. Virus and worms- These are the oldest form of cybersecurity threats. They include malicious programs which replicate themselves often causing data loss or corruption of system.
2. Man-in-Middle attacks- Manipulation and interception of data while it is travelling from one node to another to steal sensitive data.
3. Phishing-A social engineering attack in which a person is tricked into revealing personal information to steal data typically account details.
4. Brute force attacks-Attackers use brute force method to crack password of the application to access data or manipulate it
5. Trojan horses- Malicious software are disguised at legitimate sources to tricks users into accessing them which may lead to hacking of devices and data loss.

As the technology advanced, attackers have also taken a new approach to deploy their attacks. Some of such attacks include: -

1. Automated phishing- AI- made emails are being used to trick people which look very convincing hence increasing the chances of people falling prey to it.
2. Zero-day exploits- The attacks that are deployed on previously known vulnerabilities before developer can release patches.
3. Cloud and IOT based threats-Hijacking unsecure IOT devices to launch various devices such as DDOS or data theft has proven to be fatal. Cloud environment intrusions increased by 75% over the past year
4. Wireless Malware-Instead of deploying malware files to corrupt the system, attackers exploit built-in system tools.



From 2009 to 2019, the frequency of cyber-attack occurrences resulting in financial damages over $1 million increased, as seen in the chart below. From 2009 to 2015, the frequency of such occurrences ranged between 20 and 32 per year, demonstrating rather stable cyber threat activity. However, beginning in 2016, the numbers increased substantially, hitting 66 in 2017, 104 in 2018, and 105 in 2019. This dramatic increase demonstrates the increasing sophistication and financial impact of cyber threats, which are most likely being driven by the rise of ransomware, advanced persistent threats (APTs), and large-scale data breaches. The trend emphasizes the critical need for enhanced cybersecurity measures, proactive threat intelligence, and investment in cyber defense strategies to reduce financial and operational risks for enterprises and organizations around the world. Since 2001, the victim count has increased from 6 victims per hour to 97, a 1517% increase over 20 years.

II. HUMAN ELEMENT IN CYBER THREATS

Human factor in cyber threats is one of the most important yet underrated parts of cybersecurity. Over the years, this has remained the most significant vulnerability. It accounts for 82% of thefts or breaches arising from social engineering attacks, errors due to weak passwords, or sharing SPILs (sensitive Personal Identifiable Information). And still, technology notwithstanding, human beings are the weakest part of the security chain.

Cybercriminals exploit human psychology rather than merely attacking from the technical perspective. All of this takes the form of social engineering criminal attacks like phishing, baiting, and pretexting and drives unsuspecting people into receiving confidential information or opening links that are malicious. Adversaries prey on emotional weaknesses in individuals, like fear, constrained time, or bucketloads of curiosity, to bypass even high-security systems. Insider threat turns to be that much high risk when employees and contractors or business partners unknowingly or intentionally put the security at serious risk. An employee may steal confidential information, while an unwittingly offensive employee may unintentionally leak sensitive information. Mixing more adverse cybersecurity behaviors complicates the situation further. Remote offices and hybrid office concepts have also enlarged the attack surface since users are connecting to the corporate networks on public devices and networks. Inadequate cybersecurity knowledge and training are also some important concerns as people do not always understand threats and best practices for keeping information secure.

Organizations should invest in continuous security awareness training programs, put strict access control measures, and create a culture of "people security" to reduce the punishment of human factor threats. Technology can afford strong protections, but at the end of the day, cybersecurity belongs to everyone, needing a combination of technical controls and informed, watchful users. By addressing this human factor, cyber organizations have greatly managed to reduce the risk factor of cyber-attacks and increase their overall security posture.

III. LITERATURE REVIEW

1. The New Frontier of Cybersecurity: Emerging Threats and Innovations by D. Dave, G. Sawhney, P. Aggarwal, N. Silswal and D. Khut, categorized security threats into four primary categories - malware attacks, social engineering attacks, network vulnerabilities, and data breaches. It also emphasized the effects of such threats on individuals, company and society as a whole.[1]

2. Mitigation Strategies for IoT Attacks Using Blockchain: A Survey by D. Balakotaiah and D. R. Rani, emphasized the need for cybersecurity while using IOT devices as they are most vulnerable to attacks due to data transfer across devices. It also states the fact that Blockchain technology can not be implemented to all IOT devices due to limited resources.[2]

3. A survey of emerging threats in cybersecurity by Julian Jang-Jaccard, Surya Nepal, presented most exploited vulnerabilities and the techniques used to mitigate them and whether they work or not. It also showcased emerging threats along with new technologies.[3]

4. Emerging Cyber Security Threats and Security Applications in Digital Era by Pulkit Sharma, Himanshu Gupta, looks at new security threats and exposes their complexities while using several case studies from real life and the losses suffered by individuals and companies involved. [4]

5. Foresight of cyber security threat drivers and affecting technologies by Yoel Raban, Aharon Hauptman, included surveys in their study to focused on both aspects of cyber- attacks which include the factors that make a system vulnerable to attacks and the technologies that can be used to eliminate such threats and vulnerabilities.[5]

6. A critical review of emerging cybersecurity threats in financial technologies By Uchenna Joseph Umoga , Enoch Oluwademilade Sodiya , Olukunle Oladipupo Amoo and Akoh Atadoga provides a thorough review of both traditional and emerging cybersecurity threats in FinTech. The paper also highlights how FinTech's interconnected nature amplifies the impact of cyber threats, emphasizing the potential for large-scale disruptions and also includes the human factor in both psychological and behavioral aspects.[6]

7. Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses by Fnu Jimmy explores the idea of how ai Analyzes vast amount of data in real time Identifying anomalies and patterns that traditional methods miss this can help in Detecting zero day attacks and polymorphic malware which are difficult to detect Ai also greatly enhances The response time efficiency and accuracy of the attacks.[7]

8. The rise of cybersecurity: threats, challenges and solutions by Marin CLIMA, Catalin DARZU, Vasile PASCARI*, Andrei BOBEICA tackles a wide variety of cybersecurity topics such as threats that is malware fishing ransomware ddos, emerging trends that is AIIOT 5G and challenges such as skill gap regulatory compliance geopolitical issues also the inclusion of real life case studies and emphasis on robust security measures including emphasis on proactive defense highlighting the importance of continuous monitoring threat intelligence and advanced security technologies.[8]

9. Advancements in Cybersecurity: Novel Approaches to Protecting Against Emerging Threats and Vulnerabilities by Atheer Alaa Hammad1 , Hadeel M Saleh2,3* , and Mohammed F. Alomari4,5 provides a detailed walkthrough of growing threat landscape particularly Concerning Internet of things and artificial intelligence it also offers comprehensive analysis of security risks associated with the same the paper also discusses approaches like zero trust architecture and deception technologies providing insights into their implementation and potential benefits it also examines the role of Blockchain and quantum cryptography in enhancing cybersecurity.[9]

10. Advanced Cyber Threats and Cybersecurity Innovation: Strategic Approaches and Emerging Solutions by Jobanpreet Kaur1, Syed Nazmul Hasan1 ✉, Shuchona Malek Orthi2, Md Alamgir Miah3, Mohammad Abdul Goffer3, Clinton Ronjon Barikdar3, Jahid Hassan3 covers a wide range of latest cybersecurity threats including ai driven attacks, ransomware evolution and zero day vulnerabilities and also the emerging technologies such as blockchain, zero trust architecture the paper also focuses on pressing cybersecurity concerns and

recent events such as colonial pipeline attack which adds context to the paper.[10]

11. Cyber Security Challenges and its Emerging Trends on Latest Technologies by Dr.Prof. Rajasekharaiah K.M1 , Chhaya S Dule2 ,Sudarshan E3 highlights current issues in cybersecurity such as phishing attacks, iot ransomware and mobile security threats making it highly relevant. The paper also provides an overview of various cybersecurity techniques such as firewalls malware scanners and authentication methods which help in understanding basic cybersecurity defenses. The paper also discusses risks associated with social media which is of a huge concern in modern cybersecurity.[11]

12. Cyber security: contemporary cyber threats and national strategies by Zahid Oruj provides comprehensive from general concept of digital transformation to specific national cybersecurity strategies, the paper also includes technical legal and strategic aspects of various countries which provides a comparative perspective. the paper also discusses industry 4.0, IOT and other emerging technologies which underscores the urgency of cybersecurity threats.[12]

13. Comprehensive Cybersecurity Review: Modern Threats and Innovative Defense Approaches by Shrouk El-Amir has a wide coverage in relevance to cybersecurity such as threat actors, attack methods, defense strategies, malware, ransomware, phishing, zero trust models etc. also the inclusion of real-world case studies, such as the Colonial Pipeline and Accellion data breaches, adds practical context.[13]

14. Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection by Juan E. Rubio, Rodrigo Roman, Javier Lopez provides a detailed view of industry 4.0 based on IETF standard 7416 the paper covers both general and specific cybersecurity threats arising from industry 4.0 enabling technologies such as IoT, Cloud/Fog Computing, Big Data, and Virtualization.[14]

15. Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection by Rafiul Azim Jowarder * and Sawgat Jahan thoroughly examines various cybersecurity risks posed by quantum computing, including encryption vulnerabilities, data decryption risks, and Shor's and Grover's algorithms impact cryptographic protocols. the paper also provides solutions to post quantum computing cryptography techniques such as lattice-based, code-based, multivariate polynomial, and hash-based cryptography.[15]

IV. FRAMEWORKS USED TO PREVENT CYBER THREATS

Various organizations have been focused on building frameworks which have proven useful in improving security of system against cyber-crimes. Some frameworks used to strengthen security of system are: -

1. NIST Cybersecurity Framework- It was developed for industries to identify, access and eliminate the risks. It works on five core components- Identify, Protect, Detect, Respond, Recover. It is widely used by government organizations as well as private companies.

2. ISO/IEC 27001 & 27002- It is used to establish best practices for information security systems. It has two main components- ISO 27001, ISO 27002. It can be used of companies of all sizes.

3. CIS(Centre of Internet Security) Controls- Defines 18 security controls that prove useful to defend against cyber-security risks. It's main components include- data protection, account management, access control management audit log management etc. It is used for actionable best security practices.

4. OWASP Framework (Open Web Application Security Project)- It is one the most famous security frameworks. Focuses on web application security along with that it has a list named-OWASP top 10 list which is updated regularly according to new vulnerabilities. Helps developers and business owners to improve web security

5. Zero Trust Architecture (ZTA)- It focuses on enforcing the principle that individuals must be given minimum access to resources to protect resources. As most attacks are caused due to human ignorance, implementing this method can surely increase security of system. It can be used by cloud service organizers and government agencies.

V. TECHNEIQUES TO REDUCE CYBER-SECURITY THREATS

As cyber-threats have been an issue from a long time various methods have been developed to combat these threats. As most of the threats are caused due to human effect, enforcing secure software development practices and adhering to frameworks can reduce the number of cybersecurity attacks by a huge margin. Training and awareness amongst employees about social engineering attacks and teaching them about safe practices can prove to be very useful.

As cyber-threats have been an issue from a long time various methods have been developed to combat these threats. As most of the threats are caused due to human effect, enforcing secure software development practices and adhering to frameworks can reduce the number of cybersecurity attacks by a huge margin. Training and awareness amongst employees about social engineering attacks and teaching them about safe practices can prove to be very useful.

Data encryption is being used by all major applications where data needs to be transferred from one device to another. It is very beneficial in preventing Man-In-Middle attacks and ransomware. It also helps in maintain integrity of data being transferred. Having a playbook which contains methods used in past to recover damage caused by cybersecurity attacks can help employees in recovering system efficiently and in much lesser time.

VI. INNOVATION IN CYBERSECURITY

A number of ground-breaking developments are anticipated to revolutionize how individuals and organizations protect their digital assets and react to new cyberthreats as 2025 draws near.

This article examines the developments that have the potential to revolutionize cybersecurity, along with their possible ramifications and difficulties.

1. Artificial Intelligence for Real time threat detection-AI's role in cybersecurity has grown exponentially and it is expected to be $726.63 billion by 2028. Earlier live video recordings or human surveillance was used to monitor real time traffic and detect any suspicious behavior but recently this role has been shifted to AI.AI's ability to process large dataset at a high speed is very beneficial in detecting abnormal activity that may signify any kind of cyberattack. It increases speed and accuracy of threat detection and reduces the dependence on human efforts.

2. Blockchain for decentralized security- Although blockchain is most known for its use in cryptocurrency, its potential in cybersecurity is becoming more widely acknowledged. It is the best option for protecting sensitive information and systems since it can produce tamper- proof records. Blockchain can safeguard Internet of Things (IoT) devices and lessen network vulnerabilities. Blockchain guarantees transparency, decentralization, and fraud protection with its unchangeable ledger. Additionally, because blockchain is decentralized, it is immune to attacks that target centralized databases, which is a popular strategy in cyberwarfare.

3. Quantum Cryptography- Utilizing the concepts of quantum mechanics, quantum cryptography is a sophisticated type of cryptographic security that produces unbreakable encryption. Since quantum cryptography is based on the principles of physics rather than mathematical complexity, it is theoretically impervious to hacking, even by quantum computers, in contrast to standard cryptography techniques.

4. Advanced biometric authentication- Biometric authentication has been in trend since few years now. Now even typing speed and mouse movements are being used to verify identity. Ears are being scanned for optimized result as it has proved to be 97% effective which makes them highly resistant to impersonation or theft.

VII. DRAWBACKS

Even after being highly effective in preventing cyber security threats, new methods have several drawbacks which are as following: -

1. Most of the cybersecurity risks and attacks occur due to human error such as phishing or weak password. These errors cannot be completely eliminated with the assistance of automated

techniques. Relying too much on AI systems can give false sense of security and may lead to increased human error.

2. Implementing AI-driven threat detection can lead to serious risks if attacker tries to manipulate AI systems. Furthermore, applying this technique requires investments and experience. Thus, implementation is not feasible for small sized companies.

3. AI-driven security may raise ethical concerns related to user privacy. Government and Companies may misuse cybersecurity techniques to obtain confidential data or for surveillance.

4. Although effective, new cybersecurity innovations can be quite expensive. Regularly training employees about new vulnerabilities may prove to be a costly and time- consuming task.

5. Advanced security solutions may prove efficient towards current attacks but as the counter measures advance so, do the methods employed by attackers. Thus there is constant need of updating the methods.

VIII. CONCLUSION

The rapid development of technology has established a cybersecurity landscape that is constantly evolving, new threats emerging as fast as there are new solutions. With businesses, governments, and individuals increasingly dependent on the internet, the cybercriminal's attack surface only continues to expand. The emergence of artificial intelligence (AI), the Internet of Things (IoT), and cloud computing has brought unprecedented opportunities as well as major security threats. Ransomware, phishing, advanced persistent threats (APTs), and zero-day exploits remain evolving threats as they use clever attack vectors that outwit even the most sophisticated security infrastructure. Also, as more and more malicious actors deploy AI and automation, cyberattacks can be launched on a far larger scale and with greater efficiency.

While cybersecurity technologies will be evolving at an equally fast pace to counter these threats, AI-driven threat intelligence, behavioral analytics, and blockchain are enabling organizations to adopt a more proactive approach to responding to attacks. In no small way, Zero Trust Architecture is creating a new security apparatus by constantly verifying the user identity and authorizing extremely granular access. Among the various threats posed by quantum computing is the disruption of traditional cryptosystems, but it also represents opportunities because there are new types of quantum-resistant encryption. Cybersecurity frameworks are being made stronger. However, despite technological progress, the human factor remains the most significant vulnerability in cybersecurity

The future will continuously present an unending tussle between attackers and defenders. It requires collaboration with governments, private enterprises, and security researchers to save the world from the laps of the endless evolving threats in the cyber-resilient model.

REFERENCES

[1] Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023, November). The new frontier of cybersecurity: emerging threats and innovations. In 2023 29th International Conference on Telecommunications (ICT) (pp. 1-6). IEEE.

[2] Balakotaiah, D., & Rani, D. R. (2024, December). Mitigation Strategies for IoT Attacks Using Blockchain: A Survey. In *2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)* (pp. 282-288). IEEE.

[3] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences*, *80*(5), 973-993.

[4] Sharma, P., & Gupta, H. (2024, March). Emerging Cyber Security Threats and Security Applications in Digital Era. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-6). IEEE.

[5] Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *foresight*, *20*(4), 353-363.

[6] Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial

technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.

[7] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74.

[8] CLIMA, M., DARZU, C., PASCARI, V., & BOBEICA, A. (2024). The rise of cybersecurity: threats, challenges and solutions.

[9] Hammad, A., Saleh, H., & Alomari, M. (2024). Advancements in Cybersecurity: Novel Approaches to Protecting Against Emerging Threats and Vulnerabilities. *CyberSystem Journal*, *1*(1), 9-23.

[10] Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced Cyber Threats and Cybersecurity Innovation-Strategic Approaches and Emerging Solutions. *Journal of Computer Science and Technology Studies*, *5*(3), 112-121.

[11] Naik, L. B. (2022). Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *International J. Sci. Res. Eng. Manag.*, *6*(06).

[12] Oruj, Z. (2023). Cyber Security: contemporary cyber threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*, (2), 100-116.

[13] El-Amir, S. (2023). Comprehensive Cybersecurity Review: Modern Threats and Innovative Defense Approaches. *International Journal of Computers and Informatics (Zagazig University)*, *1*, 30-37.

[14] Rubio, J. E., Roman, R., & Lopez, J. (2017, October). Analysis of cybersecurity threats in industry 4.0: the case of intrusion detection. In *International conference on critical information infrastructures security* (pp. 119-130). Cham: Springer International Publishing.

[15] Jowarder, R. A., & Jahan, S. (2024). Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection. *World Journal of Advanced Engineering Technology and Sciences*, *13*(1), 330-339.