Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
April to June 2024, E-Journal, Vol. I, Issue XLVI, ISO 9001:2015 - E2024049304 (QMS)

Emerging Technologies in Cyber Security- How Best to Protect us from Cyber Threats

Sudhish Kumar*

***Asst. Prof. (Maths.) Govt. College, Khurai, Distt. Sagar (M.P.) INDIA**

Abstract - The concept of cybersecurity refers to cracking the security mechanisms that break in dynamic environments. In present days there is race between cyber threats and the mechanism of cyber security. With the advent of AI (artificial intelligence), chat GPT, machine learning data analyticswe are living in the world in the fast changing world of virtual reality. Most of us and our systems in working environment regularly face ever increasing threat of cyberbreaches and crimes and our bank accounts and as well as our children are exposed to hackers and cyber criminals. In this research paper we analyze the importance of use of modern technologies for the purpose of cyber security in a lucid manner and other related topics like ethical hacking.

Introduction - In the ever-evolving landscape of digital innovation, the surge of emerging technologies brings both unprecedented opportunities and formidable challenges, particularly in the realm of cyber security. While cyberattacks themselves are becoming more sophisticated, the rapid growth of emerging technologies such as 5G, robotic process automation and, of course, generative AI, means there are even more opportunities for cyberattacks and data breaches to occur. This blog post aims to unravel the complex dynamics of emerging technologies, such as quantum computing, artificial intelligence, cloud computing, and their profound impact on cyber security strategies and practices. We will explore how these technologies are reshaping threat landscapes, introducing new vulnerabilities, and simultaneously offering novel solutions to protect our increasingly interconnected world.

Quantum Computing, 5G Networks, and Edge Computing Emerging technologies such as quantum computing, 5G networks, and edge computing are accelerating at a rapid pace. Each of these technologies introduces distinct cyber security challenges:

Quantum Computing:

- **Encryption Vulnerabilities:** Quantum computers pose a threat to commonly used encryption algorithms like RSA and ECC, jeopardizing the privacy and integrity of sensitive data, including financial transactions and personal information.
- **Post-Quantum Cryptography:** The development and implementation of quantum-resistant cryptographic algorithms are essential to maintain secure communication in the quantum era.
- **5G Networks:**
- **Increased Attack Surface:** The expansive deployment of 5G networks amplifies the attack surface, encompassing more devices and higher data transmission volumes.
- **Network Slicing and Virtualization:** These features of 5G introduce new vulnerabilities, necessitating effective segmentation and isolation to prevent unauthorized access and data breaches.

Edge Computing:

- **Distributed Security:** The decentralized nature of edge computing demands consistent security measures across various nodes, including securing edge devices and communication channels.
- **Latency and Bandwidth Constraints:** Balancing security with the need for low-latency and real-time processing is crucial in edge computing environments .

Artificial Intelligence (AI) and Machine Learning (ML):- AI and ML are increasingly integral to cyber security, enhancing threat detection and security task automation. However, they also present unique challenges as AI is being used to create more advanced and sophisticated cyber attacks:

- **Misinformation and Disinformation:** AI's ability to generate human-like responses can be exploited to spread false information.
- **Phishing and Social Engineering:** AI-enhanced campaigns can deceive users into divulging sensitive information.
- **Bias and Unfair Representation:** AI algorithms can inherit biases from their training data, potentially leading to unfair or discriminatory outcomes.
- **Privacy and Data Protection:** Ensuring the security of personal and sensitive data shared with AI models is

paramount .

Cloud Computing: Cloud computing has seen significant adoption, with 93% of technology leaders in 2022 identifying as "mostly cloud." Securing cloud environments, however, remains a challenge:

- **Identity and Access Management (IAM):** Implementing strong IAM practices is essential for controlling access to cloud resources.
- **Data Loss Prevention (DLP):** Techniques like data classification and policy enforcement are crucial to prevent unauthorized data disclosure.
- **Incident Response and Forensics:** Developing specific incident response plans for cloud environments is necessary to effectively address security incidents .

Protection against cyber security challenges posed by emerging technologies

1. **Invest in Quantum-Resistant Encryption:** To counter the threat of quantum computing, organizations should invest in developing and adopting quantum-resistant encryption methods. This will help secure data against future quantum attacks.
2. **Robust Network Security for 5G:** Implement advanced security protocols and continuous monitoring systems to protect against the increased vulnerabilities of 5G networks. This includes the use of next-generation firewalls, intrusion detection systems, and regular security audits.
3. **Secure Edge Computing Infrastructure:** Establish strong security protocols at every node of the edge computing infrastructure. This should include regular updates, patch management, and secure authentication methods to protect against distributed security threats.
4. **Ethical AI and ML Practices:** Implement ethical guidelines and rigorous testing for AI and ML models to avoid biases and potential misuse. Regularly update these models to respond to new threats and ensure they are trained on diverse, unbiased data sets.
5. **Enhanced Cloud Security Measures:** Adopt a comprehensive cloud security strategy that includes strong identity and access management (IAM) controls, data loss prevention (DLP) systems, and an effective incident response plan tailored for cloud environments.
6. **Employee Training and Awareness:** Regularly train employees on cyber security best practices and the latest threats. This human element is crucial in defending against social engineering attacks and ensuring responsible use of technology.
7. **Regular Security Audits and Assessments:** Conduct regular security audits and risk assessments to identify and address vulnerabilities in the organization's cyber security infrastructure, particularly in areas affected by emerging technologies.

The integration of these emerging technologies in cyber security offers tremendous opportunities for innovation and efficiency. However, they also raise significant concerns about security, privacy, and data integrity. It is essential to prioritise research, development, and the implementation of advanced security measures to address these evolving challenges. Additionally, in 2022, a staggering 76% of organisations experienced a ransomware attack, indicating the increasing sophistication of cyberthreats and the urgent need for adaptive cybersecurity strategies . In this dynamic environment, staying updated on emerging technologies and their implications is critical for building robust, effective cyber security defences.

Organizations in all sectors worry about cybersecurity threats. In 2021, businesses experienced 50% more cyberattacks each week compared to 2020. Experts and researchers must constantly create new cybersecurity tools, techniques, and practices.

This page looks at the impact of cybersecurity threats and explores the latest trends in cybersecurity technology. We cover cloud encryption, extended detection and response, and context-aware security. We also examine defensive AI, manufacturer usage description, and zero trust.

Impact of Current and Emerging Cybersecurity Threats: Cybersecurity threats impact businesses, government, nonprofit groups, and people. Researchers and information security experts work regularly to create proactive methods and tools to improve cybersecurity.

Ransomware attacks and weaknesses from increased cloud service use are some emerging threats. Potential vulnerabilities of 5G technology and the evolution of the Internet of Things (IoT), which includes smart home devices, also pose securityrisks.

Today's New Cybersecurity Technologies: Below, we describe some of the most popular cybersecurity technologies in the field. We cover how they work and their applications in cybersecurity. Cybersecurity experts use these tools to defend against the cyberthreats described above.

Cybersecurity threats can stimulate the development of new cybersecurity technology. Read on for details about some of the most promising new technologies created to fight current cybersecurity threats.

Behavioural Analytics: Behavioural analytics looks at data to understand how people behave on websites, mobile applications, systems, and networks. Cybersecurity professionals can use behavioural analytics platforms to find potential threats and vulnerabilities.

Analysing patterns of behaviour can lead to identifying unusual events and actions that may indicate cybersecurity threats.

For example, behavioural analytics may find that unusually large amounts of data are coming from one device. This may mean a cyberattack is looming or actively happening. Other indicators of malicious activity include odd timing of events and actions that happen in an unusual sequence.

Benefits of using behavioural analytics include early detection of potential attacks and the ability to predict future attacks. Organizations can automate detection and response using behavioral analytics.

Blockchain: Blockchain is a type of database that securely stores data in blocks. It connects the blocks through cryptography. Blockchain allows information to be collected, but not edited or deleted.

Cybersecurity professionals can use blockchain to secure systems or devices, create standard security protocols, and make it almost impossible for hackers to penetrate databases.

Benefits of blockchain include better user privacy, reduction of human error, greater transparency, and cost savings by removing the need for third-party verification.

Blockchain also eliminates the security problem of storing data in one place. Instead, data gets stored across networks, resulting in a decentralized system that is less vulnerable to hackers.

Challenges of using blockchain include the cost and inefficiency of the technology.

Cloud Encryption: Cloud services improve efficiency, help organizations offer improved remote services, and save money. However, storing data remotely in the cloud can increase data vulnerabilities. Cloud encryption technology changes data from understandable information into an unreadable code before it goes into the cloud.

Cybersecurity professionals use a mathematical algorithm to complete cloud encryption. Only authorized users with an encryption key can unlock the code, making data readable again. This restricted access minimizes the chance of data breaches by unauthorized attackers.

Experts agree that cloud encryption is an excellent cybersecurity technology for securing data. Cloud encryption can prevent unauthorized users from gaining access to usable data. Cloud encryption can also foster customer trust in cloud services and make it easier for companies to comply with government regulations.

Context-Aware Security: Context-aware security is a type of cybersecurity technology that helps businesses make better security decisions in real time.

Traditional cybersecurity technologies assess whether or not to allow someone access to a system or data by asking yes/no questions. This simple process can cause some legitimate users to be denied, slowing productivity.

Context-aware security reduces the chance of denying entry to an authorized user. Instead of relying on answers to static yes/no questions, context-aware security uses various supportive information like time, location, and URL reputation to assess whether a user is legitimate or not.

Context-aware security streamlines data-accessing processes and makes it easier for legitimate users to do their work. However, end-user privacy concerns pose a challenge.

Defensive Artificial Intelligence (AI): Cybersecurity professionals can use defensive artificial intelligence (AI) to detect or stop cyberattacks. Savvy cybercriminals use technologies like offensive AI and adversarial machine learning because they are more difficult for traditional cybersecurity tools to detect.

Offensive AI includes deep fakes, false images, personas, and videos that convincingly depict people or things that never happened or do not exist. Malicious actors can use adversarial machine learning to trick machines into malfunctioning by giving them incorrect data.

Cybersecurity professionals can use defensive AI to detect and stop offensive AI from measuring, testing, and learning how the system or network functions.

Defensive AI can strengthen algorithms, making them more difficult to break. Cybersecurity researchers can conduct harsher vulnerability tests on machine learning models.

Extended Detection and Response (XDR): Extended detection and response (XDR) is a type of advanced cybersecurity technology that detects and responds to security threats and incidents. XDR responds across endpoints, the cloud, and networks. It evolved from the simpler traditional endpoint detection and response.

XDR provides a more holistic picture, making connections between data in different places. This technology allows cybersecurity professionals to detect and analyse threats from a higher, automated level. This can help prevent or minimize current and future data breaches across an organization's entire ecosystem of assets.

Cybersecurity professionals can use XDR to respond to and detect targeted attacks, automatically confirm and correlate alerts, and create comprehensive analytics. Benefits of XDR include automation of repetitive tasks, strong automated detection, and reducing the number of incidents that need investigation.

Manufacturer Usage Description (MUD): Manufacturer usage description (MUD) is a standard created by the Internet Engineering Task Force to strengthen security for IoT devices in small business and home networks.

IoT devices are vulnerable to network-based attacks. These attacks can lead to loss of private data or cause a machine to stop working properly. IoT devices need to be secure without costing too much or being too complicated.

Benefits of using MUD include simply, affordable improved security for IoT devices. Cybersecurity professionals can use MUD to make devices more secure against distributed denial of service attacks. MUD can help reduce the amount of damage and data loss in the event of a successful attack.

Zero Trust: Traditional network security followed the motto "trust but verify," assuming that users within an organization's network perimeter were not malicious threats. Zero Trust, on the other hand, aligns itself with the motto, "never trust, always verify."

A framework for approaching network security, Zero

Trust makes all users authenticate themselves before they get access to an organization's data or applications.

Zero Trust does not assume that users inside the network are more trustworthy than anyone else. This stricter scrutiny on all users can result in greater overall information security for the organization.

Cybersecurity professionals can use Zero Trust to deal more safely with remote workers and challenges like ransomware threats. A Zero Trust framework may combine various tools, including multi-factor authentication, data encryption, and endpoint security.

Regulation: As the frequency of cyberattacks continues to grow significantly each year, governments are beginning to use and promote best practice regulations. In the past, the governments did not often get involved in cybersecurity issues.

Security Magazine, an industry publication for cybersecurity professionals, predicts that 2022 will be the year that governments start to play a bigger role in regulating how organizations ensure user information security.

Potential regulatory changes include executive orders regarding cybersecurity standards for government suppliers, penalties for companies that do not engage in best practices, increased demand for cyber insurance, and ransomware disclosure laws. Greater regulation will likely lead to improved security standards.

Organizations Researching Cybersecurity Technology: The following list of organizations conduct research on cybersecurity technology and trends. Visit these websites to stay informed about the latest developments in the field.

- **Computer Science and Artificial Intelligence Laboratory:** Massachusetts Institute of Technology's CSAIL conducts computing research to improve life and help machinesoperate more efficiently and effectively. The organization of more than 60 researchgroups creates new technologies. The group works with an annual budget of more than$65 million.
- **Cyber Security and Privacy Research Institute:** An interdisciplinary research instituteat George Washington's School of Engineering & Applied Science, CSPRI coordinatesresearch, conferences, and campus dialogue on cybersecurity and privacy. The instituteworks with private organizations and government agencies. Research topics include foodchain security, K-12 cyberlearning, and the gender gap in cybersecurity careers.
- **Institute for Information Security & Privacy:** Georgia Tech's School of Cybersecurityand Privacy's IISP serves as a starting point for 13 cybersecurity labs, centers, andfacilities. Faculty and students work in cybersecurity projects focused on resilient military cyber defense, embedded systems, and data mining. The institute includes200,000 square feet of classified research space.
- **National Cybersecurity Center of Excellence:** The NCCoE includes government, industry, and academia dedicated to protecting the nation's infrastructure and securing ITsystems. Featured projects explore 5G cybersecurity, data classification, andcryptography. Participants can make technical contributions, join a community of interest, and engage academically.
- **Rand Corporation:** The Rand Corporation focuses on improving decision making andpolicy through research and analysis in diverse research areas, including cybersecurity. Cybersecurity research explores topics like preparing for cyberattacks at the local level, extremism online, and detecting U.S. government cyber vulnerabilities. Find reports, brochures, and multimedia research resources on the group's website.

Conclusion: Thus we can safely conclude that the war against cyber threats posed by cyber criminals eyeing our money and our vulnerable children can best and who make misuse of modern technologies can best be fought and won by intelligent use of available modern technologies.

Reference:-

1. We have used open ended study material freely available on the topic of cyber security on internet.

****