Review on Emerging Technologies and Security Challenges

Amir Khosru
2114951058@uits.edu.bd
Dhaka
University of Information Technology and Science(UITS)

Md. Esha Ali Emon
2114951017@uits.edu.bd
Dhaka
University of Information Technology and Sciences(UITS)

January 6, 2025

Abstract

The advent of emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and Blockchain has brought about revolutionary changes across various sectors. However, these advancements come with significant security challenges. Today, due to the modern life style people have joined technology life and using more technology for shopping as well as financial transactions in their cyber space. 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. The information security has become one of today's main challenges. Whenever we think of cyber security, we first of all think of 'cybercrimes,' which expand tremendously every day. This paper reviews the current landscape of emerging technologies, the associated security risks, and the strategies to mitigate these challenges. The paper draws insights from three key studies to provide a comprehensive understanding of the evolving cyber threat landscape and the measures necessary to safeguard these innovations.

1 Introduction

Emerging technologies have transformed the digital ecosystem, enhancing efficiency, productivity, and connectivity. However, the proliferation of these technologies has also expanded the threat surface, exposing vulnerabilities that can be exploited by cybercriminals. This paper discusses the security implications of emerging technologies and the need for robust cybersecurity frameworks. Cyber Security Challenges have been increasing rapidly these days, it's the national security in today's world, private and government organizations ranging from small to large enterprises, government universities and private universities, hospitals, all exposed to cyber-attacks from across the world. The process of digitization in all aspects of human life, like healthcare, education, business, etc., has gradually led to the storage of all sorts of information, including sensitive data. Security, is the process of protecting the digitized information from theft or from physical damage while maintaining the confidentiality and availability of information but as technology is growing rapidly, the cybercrime rate also increases both in number and complexity. The reason behind this tremendous growth in cyber-crime is the usage of inadequate software, expired security tools, design flaws, programming errors, easily available online hacking tools, lack of awareness in public, high rates of financial returns, etc. In order to explore the vulnerabilities in the target and thereby to attack the victim, more powerful attack tools are developed by the technical attackers. Now it is necessary to get insights into the concepts of security defense mechanisms, different techniques and trending topics in the area of information security.

2 Emerging Technologies

2.1 Internet of Things (IoT)

The Internet of Things (IoT) is present in the daily lives of most individuals and corporations and is a technology that is spreading rapidly in almost every realm that it can fit itself into. The items that are interconnected within the IoT offer numerous benefits to consumers such as utility, quality of life upgrades, and productivity. The nature of most IoT devices marketing schemas like utilizing mass-production on a low-budget leaves them with very limited security protocols in place to protect the systems. The IoT connects billions of devices, from home appliances to industrial sensors, creating a vast network of interconnected systems. This connectivity, while beneficial, also presents significant security challenges. Poorly secured IoT devices are vulnerable to exploitation, as evidenced by incidents like the 2016 Mirai botnet attack. The botnet master effectively took control of thousands of IoT devices due to their poorly secured configuration and conducted a Distributed Denial of Service (DDoS) attack against a Domain Name System (DNS) provider which resulted in internet downtime for consumers in North America and Europe. Attack brought tremendous attention to the need for better security techniques to be implemented within these devices and some research has been conducted in areas such as blockchain based architecture to mitigate future attacks. With these concerns and past exploitations being noted, the software industry needs to adjust and take precautions in the future such as protecting architecture components and implementing existing manageable security controls that can alleviate some of the potential harm of these devices until more permanent security can be achieved.

2.2 Artificial Intelligence (AI)

AI systems, especially those used in critical applications like healthcare and autonomous vehicles, face unique security challenges. Issues such as data poisoning, adversarial attacks, and the black-box nature of AI algorithms complicate the task of ensuring their security and reliability. This analysis could hardly claim to focus on emerging technologies and their corresponding challenges if it failed to mention Artificial Intelligence (AI). Though not being a completely novel idea, this technology is seeing an all-time high of use cases in various applications such as decision-making algorithms, data mining, and the autonomous vehicles to name just a few. Trust is a common theme for challenges surrounding all the emerging technologies mentioned above, and in the case of AI and robotics it is no different. Within this field however, the challenge becomes particularly difficult due to the lack of human interaction and control within the black box of algorithms that allow these systems to operate and learn. Some questions researchers need to answer include: how can we build trust into such a system, how will it propagate throughout the chain of trust for the components, and how can it be used to raise concern about security implementation of AI and robotics technology? The threats associated with such systems is constantly evolving and can have an impact on citizens' health, safety, and privacy due to its widespread adoption.

2.3 Cyber Crime and its Evoiution

Cybercrime, as defined by the US Department of Justice,encompasses any illegal activity involving a computer. The rise of IoT devices, AI applications, and blockchain technologies has introduced new forms of cyber threats, including identity theft, ransomware, and advanced persistent threats. Cybercrime is a term for a crime which uses a PC mobile for robbery and crime of commission. The increasing list of cybercrimes includes computer crimes, such as the spread of network intrusions and pc-viruses, as well as the computer-based variant of established crimes such as theft, stalking, intimidation, and coercion. Often cyber-crimes in common people's language may also be defined as crimes committed using a PC and the web to steal the identity or sell an individual to victims of smuggling or stalking or disrupting operations with malicious programs. The majority of cybercrime is conducted to obtain information on individuals, businesses, or government officials. Even though these attacks do not target a physical body, they target the personal virtual body, a collection of informational data attributes that describe people and organizations on the internet. In other words, in the digital era, our virtual identities are critical aspects of daily life: our identities are stored in many governments and corporate computer databases. Cybercrime or digital criminals emphasize the importance of networked computers in people's lives, as well as its flaws in the face of established realities like personal identity.

2.4 Mobile Technologies

The proliferation of mobile devices has transformed how users interact with technology.It emphasize the importance of mobile security, particularly in protecting user data from unauthorized access and cyber-attacks. The integration of biometric security solutions is one approach to enhance mobile security.

2.5 Cloud Computing

The shift towards cloud computing has improved data accessibility and scalability. Yet, it also raises concerns about data privacy, security, and compliance. The shared responsibility model of cloud security demands that both providers and users implement stringent security measures.

3 Security Challenges

3.1 Cybercrime

Cybercrime has evolved alongside technological advancements, with attackers leveraging new tools and techniques to exploit vulnerabilities. Note that the increasing complexity of cyber threats poses significant challenges for organizations and individuals alike.

3.2 Data Privacy

Emerging technologies often collect vast amounts of personal and sensitive data. For example IoT devices (smart home systems, wearables) and AI-driven platforms continuously gather user behavior data, location, and biometric information. This leads to risks of over-surveillance, profiling, and misuse of personal information by corporations or governments. As more personal data is collected and stored, ensuring data privacy becomes paramount. The General Data Protection Regulation (GDPR) has set a precedent for data privacy laws, but compliance remains a challenge for many organizations.

3.3 Malware Scanners

A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system. The samples of malicious software systems in this field are generally sorting and noted as malware by viruses, worms, and the Trojan horses.

3.4 Access Control and Password Security

Security provided by the means of username and passwordis a simple way of providing security for the private information to preserve privacy. This means of providing security is one of the most critical cyber security initiatives.

4 Potential Solutions

4.1 Enhanced Security Protocols

Implementing robust security protocols is essential for protecting emerging technologies. This includes regular updates and patches for IoT devices and the adoption of advanced encryption methods for mobile applications.

4.2 User Education and Awareness

Raising awareness about cybersecurity risks and best practices is crucial. Organizations should invest in training programs to educate employees about potential threats and how to respond effectively.

4.3 Increased Investment in Automation

Automation technology is gaining ground in organisations by allowing underemployed cyber security teams to focus on more complex problems ,not on routine , often worldly work.In these situations, the first approach to data protection provides an ultimate defense against Cyber-attacks such as database fraud and fitness, and its profound effect on a business .It may enhance efficiency ,but skills and expertise are still necessary to minimize cyber security risk.

4.4 Collaboration and Research

Collaboration between academia, industry, and government is vital for addressing security challenges. Ongoing research into new security technologies and frameworks can help develop innovative solutions to emerging threats.

4.5 Cybersecurity Training and Awareness

Human error is a significant factor in many security breaches. Organizations must invest in cybersecurity training programs to educate employees about best practices, phishing scams, and the importance of maintaining good cyber hygienee.

4.6 Data Encryption and Cryptographic Techniques

Encryption remains a fundamental component of data security. Implementing robust cryptographic standards and ensuring proper key management are essential to protecting sensitive information from unauthorized access.

4.7 Security Information and Event Management (SIEM)

SIEM systems provide a centralized approach to monitoring and managing security incidents. By analyzing log data from various sources, SIEM solutions can detect patterns indicative of security breaches and facilitate timely responses

5 Conclusion

The integration of emerging technologies into various sectors has brought unprecedented benefits but also significant security challenges. Addressing these challenges requires a comprehensive approach that includes advanced security technologies, proactive threat management, and continuous education. By implementing these strategies, organizations can better safeguard their assets and ensure the secure deployment of innovative technologies.The rapid advancement of emerging technologies presents both opportunities and challenges in the realm of cybersecurity. As highlighted in this review, addressing the security implications of these technologies requires a multifaceted approach that includes enhanced security measures, user education, and collaborative research efforts. Future work should focus on developing adaptive security solutions that can keep pace with the evolving threat landscape.

References

Houssain Kettani, "On Security Implications of Emerging Technologies," ICEDS 2022.

K. M. Rajasekharaiah et al., "Cyber Security Challenges and its Emerging Trends on Latest Technologies," IOP Conference Series: Materials Science and Engineering, 2020.

Er. Harjasdeep Singh et al., "A Study of Cyber Security Challenges and Its Emerging Trends on the Latest Technologies," International Research Journal of Modernization in Engineering Technology and Science, 2023.