Chapter 13
Artificial Neural Network–Based Efficient Cyber Hacking Detection System Using Deep Learning Approaches

J. Christina Deva Kirubai
Bharath Institute of Higher Education and Research, India

S.Silvia Priscila
Bharath Institute of Higher Education and Research, India

ABSTRACT

Cyber hacking can be defined as the process of observing the incidents happening in a computer network or system and inspecting them for indications of possible incidents, which includes either violation or threats of violation in the policies of computer security, the allowable use of policies or the practices of maintaining standard security. CHS aid the network in automating the process of intrusion detection. CHPS is software that consists of all the abilities of the anomalies. In addition, it also strives to widen the possible incidents and cyber hacking methodologies with similar abilities. In the case of CHPS, it allows administrators to turn off prevention attributes in anomaly products, making them work as a cyber hacking system. Respectively, for compressing the benefits of both IPS and CHS, a novel term, cyber hacking, and prevention systems (CHPS), is used for all the further chapters to infer both CHS and IPS approaches. In this research, three algorithms, namely decision stump method (DSM), support vector machine (SVM), and artificial neural network (ANN), were used. From the results obtained, the proposed ANNAccuracy of 92.3%, MSE of 0.000119, Log Loss of 0.4288, and Mathews Coefficient of 0.9010 were proposed. The tool used is Jupyter Notebook, and the language used is Python.

DOI: 10.4018/979-8-3693-1355-8.ch013

INTRODUCTION

Cyber hacking, often referred to as hacking, is a term that encompasses a range of activities involving unauthorized access, manipulation, or exploitation of computer systems, networks, and digital data (Ahmed Chhipa et al., 2021). While hacking is a broad term, it is essential to note that not all hacking activities are malicious. Ethical hacking, for instance, involves authorized professionals testing systems for vulnerabilities to enhance security. However, "cyber hacking" commonly evokes the negative connotation associated with malicious activities (Akbar et al., 2023). At its core, cyber hacking involves individuals, commonly known as hackers, who use their technical skills to breach the security of computer systems and networks for various purposes (Angeline et al., 2023). These purposes can range from stealing sensitive information, disrupting services, conducting espionage, or promoting ideological or political agendas (Rajest et al., 2023a). The motivations behind cyber hacking are diverse, and hackers may operate as individuals or as part of organized groups.

One common form of cyber hacking is unauthorized access to computer systems. This could involve exploiting vulnerabilities in software, exploiting weak passwords, or using social engineering techniques to trick individuals into divulging sensitive information (Rajest et al., 2023b). Once access is gained, hackers may explore the system, escalate privileges, and exfiltrate valuable data. This unauthorized access can have severe consequences, ranging from financial losses to the compromise of personal or corporate information. Another facet of cyber hacking is the distribution of malware (Regin et al., 2023a). Malicious software, or malware, includes viruses, worms, trojan horses, ransomware, and other harmful programs (Lodha et al., 2023). Cyber hackers use various methods to deliver malware, such as email attachments, malicious links, or exploiting software vulnerabilities. Once on a system, malware can disrupt operations, steal information, or render the system unusable (Regin et al., 2023b).

Phishing, a form of social engineering, is another technique cyber hackers employ. In phishing attacks, hackers create deceptive emails, messages, or websites to trick individuals into providing sensitive information, such as login credentials or financial details. Phishing is a prevalent method because it preys on human vulnerabilities, relying on users' trust or fear to manipulate them into taking actions that benefit the attacker (Sajini et al., 2023). Hacktivism represents a distinct category of cyber hacking driven by political or ideological motivations. In hacktivist campaigns, hackers infiltrate systems to promote a social or political message. This can involve defacing websites, disrupting services, or stealing and leaking sensitive information to expose perceived injustices (Cirillo et al., 2023).

The continuous evolution of technology and the increasing interconnectivity of systems make cyberspace an attractive and challenging arena for hackers. As a response, cybersecurity measures and ethical hacking practices have also advanced to mitigate the risks associated with cyber hacking. Governments, organizations, and individuals invest in security protocols, encryption, and regular security audits to safeguard their digital assets from unauthorized access and malicious activities. In conclusion, cyber hacking encompasses various activities, from malicious intrusions into computer systems to ethical testing of security vulnerabilities. The term carries negative and positive connotations, depending on the intent behind the hacking activities. As technology advances, cybersecurity remains critical in defending against cyberhacking threats and ensuring digital information's integrity, confidentiality, and availability.

The primary focus of CHPSs is to recognize the possible intrusion. A CHPS can recognize the attacker successfully when compromised with the system and exploit the system's susceptibility. After that, CHPS sends a report based on the incident to the security user, who initiates the response action to reduce the damage caused by the incident (Banait et al., 2022). The CHPS enables the sending of log information