Chapter 3
Digital Risk Analytics Using Smart Feature Reduction and Deep Classification

Usharani Bhimavarapu
https://orcid.org/0000-0002-0246-1420
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, India

ABSTRACT

In today's hyperconnected world, cybersecurity has become a top priority due to the fact that digital threats constantly evolve in terms of complexity and frequency. Cyberattacks such as malware, phishing, denial of service, and advanced persistent threats take advantage of network, system, and user behavior vulnerabilities, resulting in financial, reputational, and operational loss. This study aims to counter the growing problem of cybersecurity threats through a robust framework for detection, mitigation, and prevention of cyber attacks. Particle Swarm Optimization (PSO) is applied for feature selection to identify the most significant attributes that are shaping attack patterns. A Bi-Stacked Artificial Neural Network (Bi-Stacked ANN) is intended to learn and identify intricate relationships within the data, providing superior accuracy and stability for multi-class attack classification. The model is tested against common performance metrics to ensure its efficacy.

DOI: 10.4018/979-8-3373-0613-1.ch003

INTRODUCTION

The increasing reliance on online platforms and internet-based systems has enormously exposed individuals, businesses, and governments to cyber threats. With increasingly sensitive information being stored and shared online, cyber attackers are continually evolving complex methods to target system vulnerabilities. Such attacks involve malware, phishing, ransomware, and social engineering, which can result in data loss, monetary loss, and reputational loss. The requirement for effective cybersecurity procedures stems from this fast-changing threat environment. Early identification of cybersecurity threats is essential to reducing harm and safeguarding critical infrastructure. Companies have to remain on guard by constantly monitoring and analyzing systems for vulnerabilities. With the rise of smart devices, the attack surface has grown wider, complicating detection further. The impact of ignoring cybersecurity can be disastrous, reaching millions of users worldwide. Thus, proactive threat identification is the first crucial step for an effective cybersecurity framework.

Reduction of cybersecurity threats is a primary goal of any cybersecurity strategy. Once threats are recognized, action must immediately be initiated to mitigate their effects or eliminate them altogether. This involves patching vulnerabilities in software, firewall configuration, network segmentation, and access control. Risk mitigation also includes periodic vulnerability scanning and security audits in order to make sure that systems are still secure. Organizations tend to follow a model of layered security to provide a series of defense layers in the face of attacks. Employee training is also a critical mitigation step, as most security breaches are caused by human error. Successful mitigation decreases downtime, protects intellectual property, and ensures operational continuity. Without these interventions, even small security holes can be attacked by exploiters. Moreover, mitigation measures need to be adaptive and scalable in order to react to evolving threats and technologies. Through mitigation of risks at all levels, organizations can develop resilience to increasingly complex cyberattacks.

Avoiding cybersecurity threats prior to occurrence is the most strategic and cost-effective way of ensuring digital security. Prevention requires architecting and deploying secure systems from scratch, including mechanisms like least privilege, robust encryption, and sound software development practices. Ongoing employee awareness sessions are crucial in the prevention of phishing and social engineering attacks. Organizations also apply real-time threat intelligence feeds to maintain a head start over cybercriminal techniques. Security policies need to be updated constantly to incorporate new vulnerabilities and attack trends. Preventive measures like intrusion prevention systems (IPS), endpoint protection, and network access control can very much lower the chances of a successful attack. Organizations can lower the load of future risk mitigation by ensuring security in system design at