RISK DETECTION AND CYBER SECURITY FOR THE SUCCESS OF CONTEMPORARY COMPUTING

Abstract

Cybercriminals have been searching for methods to take advantage of software flaws and engage in destructive activity since the dawn of the computer revolution. On computer networks and mobile devices, there are a variety of cybercrimes that attempt to violate users' data privacy every day. The world is getting more and more digitalized, which is causing security issues and a critical need for strong and cutting-edge security technologies and tactics to battle the increasingly complex complexity of cyber-attacks. The fight against cybercrime has given rise to a wide variety of machine learning approaches. We covered cyber security attacks in this article, as well as machine learning & deep learning methods that are essential for risk assessment and cyber security. According to the findings, machine learning algorithms offer more accuracy than some. According to the findings, machine learning techniques are more accurate than some deep learning approaches.

Keywords: Risk Detection, Cyber Security, SVM, NB, KNN, CNN, RF, DBN, RNN

Authors

Mrs. D.Radha
Research Scholar
Dept. of Computer Science,
Vels University
Assistant Professor
ShriKrishnaswamy College for Women
Anna Nagar, Chennai, India.

Dr. S.Prasanna
Head of the Department
Department of Computer Applications
Vels Institute of Science, Technology and Advanced Studies (VISTAS),
Chennai, India.

I. INTRODUCTION

Computer networks have quickly evolved, and they are now being employed in every industry due to a rising need. Computer networks have expanded and become more complicated as a result of these advancements. Computer networks are increasingly being employed wherever resource sharing & communication are required. Security issues are also brought up by this reliance on computer networks. The biggest difficulty now facing society is the security of networks and information systems. With simple-to-use apps, even amateur hackers may carry out successful cyber-attacks. Using readily available technologies, a variety of cyberattacks that could previously only be executed manually may now be automated. In order to defend against the assaults, several open source and proprietary intrusion prevention systems have been created. Despite these initiatives, maintaining cyber security is a difficult and dynamic process that combines a variety of human, software, and physical systems. The number of information system security lapses and cyberattacks is steadily rising. Techniques to fight these dangers are also being researched in response to the growing number of cyberattacks. Finding security flaws before attackers and taking the appropriate safeguards is one of these techniques [1].

Cybersecurity is a major worry for businesses everywhere. Organizational information and system resources are the target of cyberattacks carried out for monetary gain or for geopolitical reasons. This involves the theft of private corporate strategy plans, intellectualproperty, sensitive customer data, and crucial IT infrastructure. The development of organised criminal syndicates or nation-state paramilitary cyber organisations has altered the landscape of cyberthreats in recent years. The term "advanced persistent threats" (APTs) is increasingly used to characterise these types of organisations. APTs are becoming more advanced, assembling teams of IT professionals for specific purposes, and using military-grade cyber weapons in highly targeted assaults [2].

The modern, technologically sophisticated society is centred around digital life, which puts people at more danger of cybercrime than before. Cybercrime opened the door for potential threats to certain people or businesses, which resulted in significant financial damage. Data breaches are becoming more frequent, and the technical world has changed to include cyber security to safeguard sensitive and secret data. Cyber security was a technique used to safeguard networks, servers, computers, electronic gadgets, mobile devices, and data. Cybersecurity has also been used to protect other electrical devices from online attackers. The term electronic technology or information systems security is also often used. The important material was removed, moved, or leaked by malevolent attackers, posing a serious threat to businesses, organisations, or particular people. By ensuring the morality, availability, and confidentiality of data, cyber security assisted in defending data from attackers [3].

One of the most important elements in creating a strong system for cyber regulation within businesses and banks is the presence of an efficient and seamless way of managing all accounting activities taking into consideration the usage of contemporary computing techniques. Innovation and technology must be utilised if development and performance are to be made. The most significant change factors that have led to new company models and various economic values as well as increased competition on a local and global scale include uncertainties, the conversion of information systems, rapid scientific advancement, and

difficulties in the business climate [4]. By ensuring the morality, availability, and confidentiality of data, cyber security assisted in defending data from attackers [3].

In order to tackle cybercrime, cybersecurity has substantially improved in response to the growing variety of cyber threats. The term "cyber security" refers to a collection of technologies, technological experts, and processes that are utilised to develop security measures to protect cyberspace from cybercriminals. Cybersecurity techniques may be divided into two categories: automated cybersecurity and traditional cybersecurity. Traditional cyber security flaws that encourage cybercrimes include poor system resource configuration, inexperienced users, and limited access to secure data [5]. Automation will be the key to cyber security in the future. We urgently want automated and cutting-edge cybersecurity methods.

II. RELATED WORKS

Before examining the methodologies in order to identify the issues, customary analytical techniques, and research obstacles, BeenishUrooj et al [6] establish their key points. The article also looks at potential risk areas or places where SCADA system breaches might occur, as well as ways to protect against and get rid of risks when they appear during industrial manufacturing.

Siyakha N. Mthunzi et al. [7] provide a comprehensive overview of the situation of the cyber defense ecosystem at the moment. Further examination also reveals substantial tendencies towards bio-inspired strategies as novel approaches to issues in other sectors. The chapter makes assumptions about cyberspace and computer security using examples of natural predators that can survive their prey. Provided an old problem (Pold) and an old solution (Sold), a new issue (Pnew) can be conceptualised with new partial and, possibly, null solution provider (Snew) in the solution provider space Sold to Snew.

In order to simulate, test, and assess potential cyber-attack scenarios, Kara, S. et al. [8] built a cyber-attack simulation utilising the DEVS modelling technique. An application that replicates an attack in a virtualized environment & examines detector warnings by producing the proper intrusion detection signals has been created. As a development environment, the DEVS-Suite simulation tool was employed. The discrepancies between them were identified through comparisons with several cyber-attack simulation software.

Numerous topics pertaining to the use of ML in security have now been explored, according to Koushal Kumar et al. A lot of research has been done on the usefulness of using ML technologies in cybersecurity issues. The current difficulties that researchers in the field are facing have been noted and debated. The available datasets and methods for the effective use of ML in the field of cybersecurity are presented in the current chapter. The data are also contrasted by a number of different factors. The use of ML techniques by three well-known companies, Facebook, Microsoft, and Google, is finally investigated.

The history, structure, and substance of WP.29's cyber security law are examined by Scott McLachlan et al. [10]. We give a general overview of the procedures necessary to getcertification, talk about the major problems, gaps, and effects of implementation on key players, and offer suggestions for manufacturers and also the agencies in charge of

overseeing the process. We examine the role of non-academic sources in influencing public risk perception and, for better or worse, in driving legislative responses by placing the debate into a larger conceptual framework on risk certification.

In their research, YakubKayodeSaheed et al. [11] focused on using ML-supervised encryption method IDS for the Internet of Things. In order to prevent information from leaking onto the test data, feature scaling was done in the first step of this study technique utilising the Minimum-Maximum (min-max) notion of normalisation on the UNSW-NB15 dataset. This dataset consists of a variety of recent assaults and typical network traffic behaviours that have been classified into nine attack categories. The next step was using Principal Component Analysis to reduce dimensionality (PCA). Finally, the investigation employed six main machine learning models.

The experiences of a practitioner-researcher in leading a big international financial firm to adopt & integrate CTI to change cybersecurity-related practise and behaviour are described by James Kotsias et al. [12]. Through the change of cybersecurity practise and the enterprise-wide adoption of a unique way to packaging CTI for commercial contexts, the research gives practical knowledge on the organisational acceptance and integration of CTI. The study provides an example of medical trials as a type of action research, including its inputs, methods, and outcomes.

III. PROPOSED METHODOLOGY

Training and inference are two inherited ideas in machine learning. The enormous amount of data used in the training phase has been split up into numerous sets, including training and test datasets as well as a validation set. A machine learning algorithm learns the training data's function approximation representations. The validation sets certify the efficacy of the training procedure. The test set establishes the ultimate precision and potency of the prior data. The idea of inference is when input data is sent to a machine learning model that has been trained and put into use where the inferred output is obtained.

Regression, classifying, clustering, auto encoding, and other ideas are used in deep learning to execute learning tasks via multi-layer neural networks. Every node in the applications of many layers of various nodes receives input from the earlier layers, hence the input data serves as the representation for the output. This demonstrates how more complicated many linked neurons are.

1. **Machine Learning and Cybersecurity: Various Issues:** Cybersecurity is just one of the countless uses for ML models that numerous companies across the world have expressed a strong interest in adopting. In contrast to conventional cybersecurity systems, the main goal of Applications in the information security program is to increase the efficiency and automate the security analysis process. Nevertheless, the constantly evolving nature of cyber - attacks forces security researchers to investigate all potential dangers in cybersecurity systems utilising ML techniques. We will cover a variety of topics in this part that are connected to various ML use concerns in cybersecurity [13].

The problems of cyber security for protecting and safeguarding are

- Information security
- Network protection
- Disaster recovery for ongoing business operations
- Mobile safety
- Identity administration
- Cloud safety
- Database and infrastructure security
- Occupational safety
- Security education for end users

Cybersecurity has become one of the elements of organisational standards and processes as a result of the enormous financial damage caused by cyber security crimes. The hackers utilised original hacking techniques and upped their bar for attacks to one that was challenging to solve. It presented a risk to enterprises' ability to maintain data security [14].

2. **Implementation of Cyber Security in Various Organizations:** Cybersecurity has been a key strategy for protecting and supporting the network and data space in businesses. The system has to be safe and well-maintained. Various enterprises that adopted cyber security in businesses and looked at how it mitigated risks from organizations

- **Cyber security in railway industry:** The CYRAIL43 project or a shift 2 rail project are two current railway cyber security technologies (Kour, Aljumaili, Karim, &Tretten, 2019). Depending also on IEC 62443 standards in the railway industry, the researchers proposed a method for extremely high security and risk evaluation. The cloud computing industry and big data analytics, which are used to analyse and visualise the enormous amount of data on cloud platforms, are migrating alongside the internet-based railway E-Maintenance solutions. Therefore, the improvement of the cloud platform based on big data for maintenance purposes was hampered by cyber security. Additionally, the C2M2 (cyber maturity assessment model) has been chosen for assessing the cyber defense capacity of the railway sector (Kour, Karim, &Thaduri, 2020) concept explains also built a maturity model for railway enterprises.
- **Cyber security in marine organizations:** The goal of the current study was to enlighten the maritime community while making decisions about cyber security systems by thoroughly presenting marine cyber risk elements. As a result, it promoted the expansion of maritime cyber security measures by expanding insurers, operators, mariners, and regulators throughout the world. It also offered the necessary profile for marine cyber risk factors. MaCRA was useful for further study because it could be used in the actual world and because software tools improved its usefulness.
- **Cyber security in health care system:** Cyber security has recently been violated in healthcare systems, putting patients' privacy at danger and causing people to lose trust in the administration of these institutions. Although these dangers increased the risk to patients' health and financial security for healthcare companies. In order to discover the errors and remove risks from this particular company, (Bhuyan et al., 2020) investigated the primary kind of cyber defense in health organisations by choosing four actors who contributed to cyber-attacks and security [14].

3. **Machine Learning Methods for Cyber Security:** Artificial intelligence's subfield of machine learning tries to provide computers the capacity to utilise data to learn and advance without it being explicitly programmed. It makes predictions about fresh input data using mathematical models that were created by examining trends in datasets. Machine learning is used in a wide range of industries, including e-commerce, where apps are used to offer suggestions based on customer preferences and behavior, and health care, where applications are used to predict outbreaks or the likelihood that a patient will have certain diseases, like disease, based on their medical information [15].

Pattern discovery and predictive (supervised learning) algorithms are two varieties of machine learning algorithms (Unsupervised Learning). In supervised learning, an objective variable is present at all times, and a machine-learning algorithm learns to predict its value using a variety of learning approaches. By analysing the location, frequency, and timing of Web requests, a machine learning model, for example, might predict if a given IP address was used in a Distributed Denial of Service (DDOS) attack. Several machine learning methods, including Linear & Logistic Regression, Decision Trees, and Support Vector Machines, are included in supervised learning (SVM). As opposed to supervised learning, algorithms learn to detect interesting relationships or patterns in datasets, for example, utilising clustering & association algorithms to identify computer programmes, such as malware, with similar operating/behavioral tendencies [15].

- **SVMID (Support Vector Machines Based Intruder Detection):** Systems called Network Intrusion Detector (NID) are used to spot malicious network activity that compromises the privacy, integrity, or availability of a network's systems. Due to their capacity to adapt to novel and undiscovered assaults, many intrusion prevention systems are built explicitly using machine learning techniques [18].

Another popular supervised machine learning model is support vector machine (SVM). By dividing the data into two groups on both sides of the hyperplane, SVM searches for the hyperplane with the best dataset distribution. A different class is donated by each side of the hyperplane. Every data point has a class depending on which side of the hyperplane it landed on. To handle larger and noisier datasets, the support vector machine consumes a lot of time and space [5].

Based on statistical techniques and structural risk minimization, it is a powerful classifier. As it is simple to use and has high performance, it is commonly employed in categorization procedures. In order to categorise samples, SVM creates a boundaries between points in a multidimensional hyperplane. The cutoff point need to be as far away from the datasets as possible. By examining this boundary, newly contributed data are categorised [38, 62, 63]. If labelled with "xi, yi," an examples of 2 classifications of sets of data is produced in the the double space shown in Figure 6 where learned data is xi Rd, I = 1..n, yi 1, +1. Figure 6 displays the hyperplane as the thick line divider and the normal vector as w:

$$w^T xi + b \geq 1 \quad (1)$$
$$w^T xi + b \leq -1 \quad (2)$$

In the two classes linear classifier issue, the hyper plane's normal vector become w ve and the offset value b, presuming that the hyper plane distinguishes between positive and negative samples. The deciding limit is therefore the line wTx + b = 0. In this situation, it is necessary to guarantee the criteria in equations 1 and 2 [19].

Algorithm1. SVMID algorithm

- Select an algorithm using ML or DL.
- START
- Use the ML/DL algorithm to discover patterns in the data.
- Each data collection has a specified quantity of sample data gathered from it. Some sets of data have had empty lines deleted.
- Min-Max normalisation is used to normalise the data sets that were acquired.
- SVM machine learning techniques are used to classify the data sets.
- Check if someone has snuck into the class.
- Using a transformation, creating a feature set from the input space. The input space's non-linear frontiers are created by inversely transforming the separating hyperplanes' linear frontiers. The Kernel Trick technique is used.
- Use SVM modelling to regulate the flow.
- Excel the flow
- Recognize the attack and repel the perpetrator
- END IF

- **Naïve Bayes (NB):** Naive Bayes is a straightforward yet unexpectedly effective classification technique for binary (two-class) & multi-class classification issues in predictive modelling. When the method is explained using binary or category input values, it is simplest to grasp. Because the probability for each hypothesis are simplified to make their calculations tractable, it is also known as naïve Bayes or stupid Bayes [17].
- **Random Forest (RF):** Each will be used for categorization using the random forest method, which will help with the regression problems. A supervised classification algorithms may be a random forest algorithmic rule. As implied by the name, this algorithmic rule builds a forest with a variety of trees. The higher the number of trees inside the forest delivers the high accuracy outcomes in the classifier using the same methodology [17].
- **Results:** In this analysis, we used the Spambase dataset's widely used benchmark datasets to compute risk detection using deep and machine-learning learning approaches.

4. **Packet Delivery Ratio:** The Ratio of packet delivery (PDR) one of the most crucial indicators to utilise to assess system performance when malignant switching are available in a network. Figure 1 depicts how packets delivery is progressively declining or

stopping. The underlying reason for this tendency is that when data packets seek alternative channels because of timeout, packet losses grow or increase.

The quantity of packets transmitted to the destination determines the packet delivery ratio.

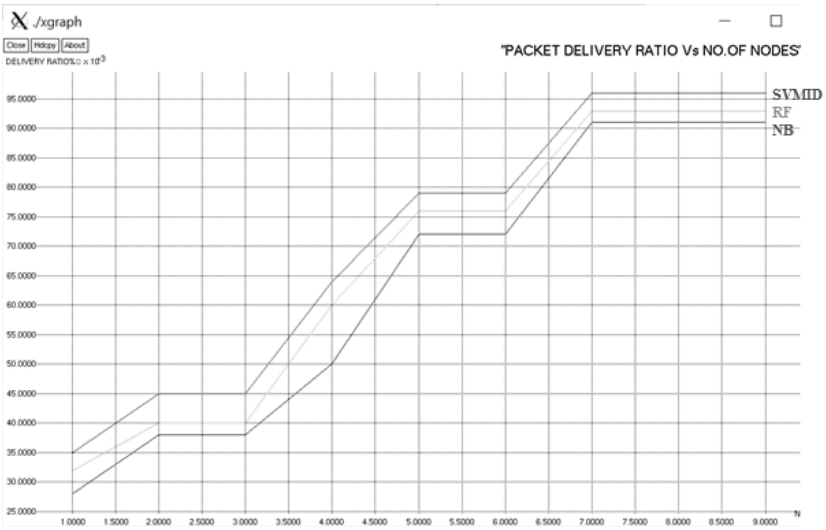

Figure1: Packet Delivery Ratio (PDR)

The accuracy is a ratio of all positively classed cases to all positively identified instances. This error rate (ERate) would be a proportion of all the dataset's occurrences that were incorrectly categorised. The recall measures the proportion of correctly categorised positive examples to all positively classified instances in the dataset.

$$\text{Precision} = TP / (TP + FP) \quad (1)$$

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (2)$$

$$\text{Recall} = TP / (TP + FN) \quad (3)$$

where FP stands for false positive, FN for false negative, TN for true negative.

Table 1

Techniques	Accuracy	Precision
SVMID	96%	95%
NB	93%	94%
RF	95%	94%

Table 1 shows the efficiency of risk detection using ML and DL algorithms in the spambase dataset.

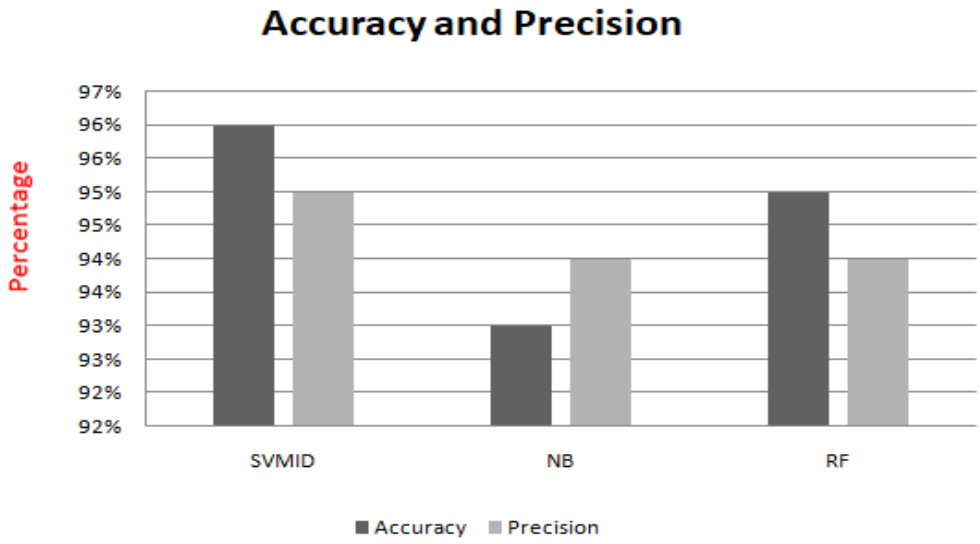

Figure 2 shows the efficiency of risk detection using the SVMID, RF, and NB algorithms in the spambase dataset.

The effectiveness of signaler in the spam baseline dataset using deep and machine learning techniques is shown in Figure 2 and Table 1. According to the findings, machine learning techniques are more accurate than some deep learning approaches. When compared to other methodologies, this Support Vector Machine based Intruder detection (SVMID) has a better accuracy rating of 96%.

IV. CONCLUSION

Deep learning and machine learning techniques are influenced by the human brain's ability to quickly learn from past experience. These techniques have been applied to tackle problems in several different study domains. Threats from the internet have increased. These assaults are beyond the capabilities of conventional security measures. Deep learning or learning algorithms are being used to overcome the limitations of conventional security systems. Cyber security is getting greater attention these days as a result of the rise in network applications and internet traffic. In this post, cyber security assaults and machine learning & deep learning techniques that are crucial for risk assessment and cyber security were discussed. Machine learning methods are in use on both the defender and attacking sides. Theresults show that machine learning methods outperform some deep learning techniques in terms of accuracy. This paper might provide as a springboard for further research that examines both the many challenges involved in establishing scaled cybersecurity systems in real-world settings as well as current security solutions.

REFERENCES

[1] Bhatia, D. (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. International Journal of Advances in Soft Computing & Its Applications, 14(1).
[2] Kotsias, J., Ahmad, A., &Scheepers, R. (2022). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 1-17.
[3] Kara, S., Hizal, S., &Zengin, A. (2022). Design and Implementation of ADevs-Based Cyber-Attack Simulator for Cyber Security. International Journal of Simulation Modelling (IJSIMM), 21(1), 53-64.

[4] Qasaimeh, G. M., &Jaradeh, H. E. (2022). The Impact Of Artificial Intelligence On The Effective Applying Of Cyber Governance In Jordanian Commercial Banks. International Journal of Technology, Innovation and Management (IJTIM), 2(1).
[5] Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020, October). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In 2020 international conference on cyber warfare and security (ICCWS) (pp. 1-6). IEEE.
[6] Urooj, B., Ullah, U., Shah, M. A., Sikandar, H. S., &Stanikzai, A. Q. (2022, September). Risk Assessment of SCADA Cyber Attack Methods: A Technical Review on Securing Automated Real-time SCADA Systems. In 2022 27th International Conference on Automation and Computing (ICAC) (pp. 1-6). IEEE.
[7] Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., & Hariri, S. (2019). A bio-inspired approach to cyber security. In Machine Learning for Computer and Cyber Security (pp. 75-104). CRC Press.
[8] Kara, S., Hizal, S., &Zengin, A. (2022). Design and Implementation of ADevs-Based Cyber-Attack Simulator for Cyber Security. International Journal of Simulation Modelling (IJSIMM), 21(1), 53-64.
[9] Kumar, K., &Pande, B. P. (2022). Applications of machine learning techniques in the realm of cybersecurity. Cyber Security and Digital Forensics, 295-315.
[10] McLachlan, S., Schafer, B., Dube, K., Kyrimi, E., & Fenton, N. (2022). Tempting the Fate of the furious: cyber security and autonomous cars. International Review of Law, Computers & Technology, 36(2), 181-201.
[11] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., &Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.
[12] Kotsias, J., Ahmad, A., &Scheepers, R. (2022). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 1-17.
[13] Kumar, K., &Pande, B. P. (2022). Applications of machine learning techniques in the realm of cybersecurity. Cyber Security and Digital Forensics, 295-315.
[14] Bhatia, D. (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. International Journal of Advances in Soft Computing & Its Applications, 14(1).
[15] Rege, M., &Mbah, R. B. K. (2018). Machine learning for cyber defense and attack. Data Analytics, 2018, 83.
[16] Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 104, 102221.
[17] Geetha, R., &Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. Archives of Computational Methods in Engineering, 28, 2861-2879.

