

Review On Machine Learning Methods To Make A Tool For Assessing CyberRisks

Abdul Khadeer, Research Scholar, Department of CSE , J.S

University, Shikohabad.

Dr. Badarla Anil ,Professor ,Supervisor, Department of CSE, J.S

University,Shikohabad.

Abstract - In the most recent decades, there has been a discernible increase in the quantity as well as the intensity of cyberattacks that are carried out on a global scale. These assaults have been having an increasingly negative effect on computer networks, computer systems, commercial businesses, and the customers of such businesses. On a yearly basis, the amount of damage they do is rising at a pace that is exponentially higher than before. In today's world, academics and businesses have come up with methods for assessing the risks posed by cybersecurity, with the objectives of identifying, estimating, and rating cyber-threats, as well as reducing the negative effects of these threats. Conventional approaches sometimes run into problems when attempting to discover indicators of unanticipated cyber threats, which limits their power to carry out exact risk assessments. The objective of this thesis is to study whether or not it is possible to use methods of machine learning with the end goal of evaluating risks associated with cybersecurity. In order to accomplish this goal, a variety of machine learning algorithms were educated, evaluated, and evaluated on synthetic datasets of varied sizes. Additionally, the current iteration of the prototype demonstrates the capacity to assist users in the process of making decisions regarding their investments in cybersecurity by incorporating

MENTOR, a recommender system for protection services. Assessments, both quantitative and qualitative, were carried out in order to determine whether or not the proposed resolution had any chance of being implemented. The findings of the quantitative analysis suggest that the prototype is capable of reaching a high level of accuracy. This conclusion can be drawn from the fact that the prototype was evaluated. On the other hand, the qualitative evaluation revealed that the suggested resolution was reliable and effective.

Key Words: risk assessments, cyber-risks, cybersecurity, qualitative evaluation.

1. INTRODUCTION

Comprehending, managing, and rating the severity of potential cyber threats are all essential steps in the risk assessment process. Because of the increasing sophistication and variety of cyberattacks, the evaluation of a business's cyber risk exposure has evolved into an essential part of the risk management strategy for that firm. It is projected that by the year 2025, these assaults would result in a loss of 10.5 trillion dollars every year in the United States. Organizations face a complicated and difficult challenge when tasked with the duty of maintaining an effective cyber risk management strategy because they must cope

with the technical improvements of cyber-adversaries as well as a rising number of exploitable vulnerabilities. The work of maintaining an effective cyber risk management plan is complex and hard. According to the results of a new poll, just 16% of executives believe that their respective firms are effectively ready to deal with cyber threats. This is despite the fact that 75% of the experts who were questioned acknowledged that cybersecurity is one of the most important concerns. In addition, the importance of devoting resources to effective governance, risk management, and compliance programs is highlighted by a research compiled by IBM that investigates the costs that are associated with data breaches. The analysis draws on data from more than 500 businesses located all over the globe.

The process of detecting, evaluating, and prioritizing possible risks and putting into action measures to avoid or mitigate the effect of such risks is referred to as risk management. It entails doing an analysis of the possible dangers that may be posed to a company or a project and devising strategies to deal with those dangers in order to prevent monetary loss, legal trouble, or damage to one's image. In order to practice successful risk management, one must have a comprehensive grasp of the risks in question, as well as the capacity to foresee possible dangers and react to them in a way that is both prompt and efficient.

The possibility of suffering a loss or being harmed is often meant to be conveyed by the word "risk" when it is used in academic writing. The phenomena often involves a certain degree of uncertainty, which makes it challenging to speculate on the outcome of the situation. According to the information shown in reference [17], several kinds of risk, such as those pertaining to business, the economy, and safety, are able to be determined based on the particular conditions. A quantitative analysis

reveals that a comprehensive risk, denoted by the letter R, may be characterized as a triplet made up of the following factors:

$$R = \langle s, p, c \rangle$$

According to the definition that was presented, a risk (R) is often made up of a scenario (s), which includes the possible adverse outcomes, the probability (p) of their occurrence, and the severity of the subsequent consequences (c), which refers to the amount of damage that is caused. In the field of information technology (IT), a risk, often referred to as a cyber-risk, is generally defined as a possible danger that has the ability to exploit a system's weaknesses, which may have detrimental effects on both financial stability and reputation. In this scenario, the manifestation of a possible danger may take the shape of cyber threats. Some examples of these include malware, ransomware, and phishing assaults, although the list is not exclusive to these. In an earlier study (reference 20), the inclusion of a knowledge component (k) into the definition of risk was proposed as a unique strategy for conceptualizing risk. This strategy was proposed as an improvement over the status quo. There is strong evidence to show that having relevant information is one of the most important factors in aiding the process of decision-making over a wide range of situations with equally likely outcomes.

Risk assessment is the necessary process of identifying, analyzing and evaluating risks. In the context of cybersecurity, the assessment process focuses on cyber-risks. Risk assessment is a key stage of the whole risk management lifecycle and in practice it includes



Figure 1: Risk management framework

The process of identifying, analyzing, and ranking the severity of prospective hazards is known as risk assessment, and it is a very important activity. The evaluation of potential dangers posed by cyberattacks is at the heart of the assessment process in the field of cybersecurity. Within the larger context of the life cycle of risk management, the activity of risk assessment serves as an essential component. It is comprised of three basic tasks, which are the analysis, appraisal, and detection of potential dangers. Figure 2.1 presents a graphical representation of an all-encompassing risk management framework for your viewing pleasure.

At its core, risk management may be seen as an ongoing process that involves assessing, mitigating, and monitoring potential dangers. The first step consists of establishing the parameters for the complete risk management approach as well as the criteria that are applied to analyze possible hazards. Following that, we move on to the evaluation stage of the process. The first stage in this phase is the identification of possible threats, which is then followed by a comprehensive inspection and evaluation of the situation. It is essential to realize that an insufficient allocation of effort during the early phase of the method for risk assessment may lead to the exclusion of prospective hazards from further analysis, which may eventually result in outcomes that were not predictable. After the risks have been ranked in order of importance, the next step is to address them according to the type, nature, and priority of each risk individually. In spite of this, developing a treatment regimen that is both rational and effective has been shown to be a difficult undertaking. In situations of this sort, having access to a comprehensive compilation of previous endeavors together with their own danger histories may make it easier to formulate more forward-thinking

remedial strategies.

In conclusion, a competent approach to risk management incorporates ongoing monitoring and surveillance in order to identify potential dangers on a regular basis. As a result, it is essential to evaluate the results after documenting and communicating them both internally (inside the team or organization) and externally (to stakeholders outside of the team or organization).

Artificial Intelligence (AI)

In theory, there are four types of AI:

Reactive Machines. These systems are considered to be the oldest type of AI and are only able to perform basic operations. More specifically, they lack memory-based functionality and therefore do not possess the ability to learn from past interactions

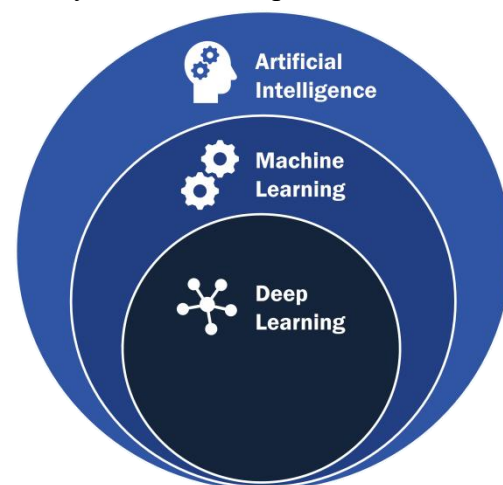


Figure 2: Artificial Intelligence overview

There are, according to one school of thought, four fundamental subfields of Artificial Intelligence (AI).

The discussion will focus on reactive machines as the subject. Rule-based systems are often recognized as the first kind of artificial intelligence; nevertheless, they only have the capabilities to carry out the most fundamental of tasks due to their restrictive

nature. To be more specific, these entities demonstrate a weakness in their capability for memory-based activities, which results in an absence of the capability to gain information from earlier encounters or events. In addition, this specific flavor of artificial intelligence can only provide a response to a limited number of inputs or a certain combination of those inputs. This limitation applies to all applications of this flavor of AI.

The idea of Limited Memory Machines is what piques people's interests at the moment. The functioning of these machines is analogous to that of reactive machines; however, in addition, these devices have the potential to learn from their previous experiences and data. After the training phase has been completed, these machines will have the ability to accurately predict and solve problems that will arise in the future. The great majority of existing applications for artificial intelligence may be functionally categorized as belonging to this specific category.

The theoretical framework of "Theory of Mind." Systems of artificial intelligence that have reached this degree of sophistication will be able to differentiate between and comprehend the feelings, needs, and cognitive processes of the persons with whom they are interacting since they will have achieved this level of sophistication. According to the claims made in this thesis, these systems are still in the infant stage and can only be found in fully autonomous cars at the current time.

The concept of self-aware artificial intelligence is what piques people's interests. At a later stage, AI systems will be able to develop the capacity for self-awareness, which is distinguished by the presence of emotions, needs, beliefs, and possibly desires.

2. THE SEC RISK AI APPROACH

Figure gives an high-level architecture overview and highlights the system components' interactions. In Step 1, the user is able to access the dashboard through any browser without the need of an account. The Graphical User Interface (GUI) (i.e., web-based interface) was designed in a way to provide total visibility of business-related KRIs and, at the same time, increase productivity and better forecasting of important aspects related to the business security. Moreover, through the web-based interface the user is able to change both contextual information and other parameters (e.g., available budget, service type and desired deployment/leasing period) required for the risk assessment and the protection service recommendations.

In order to use the information provided by the user to make risk predictions, an additional layer is required. In this approach, this task is performed by the Middleware (Step 2). More specifically, as soon as the request sent by the client is received, the Request Processor processes it and forwards the information to the Profile Evaluator, which is in charge of contacting the ML models, evaluating the prediction response, and, when specific conditions are fulfilled, establishing a connection with MENTOR (Step 6).

To perform an actual risk prediction, a request to the Risk Classifier is sent. The Risk Classifier is a prediction service included in the ML Classifier Layer (Step 3) and is essentially used to expose the trained ML models through the API. Additionally, the ML Classifier Layer also stores the trained ML models as well as the Data Scalers used to normalize the input data and increase prediction accuracy.

The process of training, validating and testing the ML models takes place in the ML workflow Layer (Step 4) and is usually carried out by data scientists/experts in the company.

In summary, the Data Generator component is used to initialize the synthetic data generation process. Afterwards, the data is processed (i.e., Data Processor) and used by the Model Builder for training, validating, testing, and building the models. Each phase

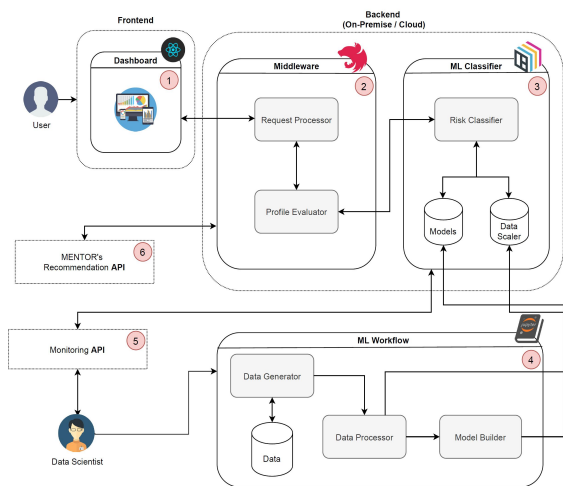


Figure 3: Architecture overview

of the ML Workflow is described with sufficient level of details in next Section. Lastly, the interface indicated by Step 5 provides a monitoring API for checking the status of the de- ployed models, retrieving model-specific metadata (e.g., version, creation time, accuracy) and other metrics about the prediction service (e.g., request duration in seconds).

The figure presents a detailed portrayal of the architecture of the system and places an emphasis on the interactions that occur between the system's many different parts. The user is able to access the dashboard with any web browser during the testing period, and creating an account is not required to do so. The Graphical User Interface (GUI), which is an interface that is based on the web, was designed with the purpose of ensuring that business-related Key Risk Indicators (KRIs) are visible in their entirety. In addition to this, it was developed to boost productivity as well

as forecasting of critical areas that relate to the safety of businesses. In addition, the user has the ability to modify contextual information as well as various parameters, such as available budget, service type, and desired deployment/leasing period, which are essential for conducting risk assessment and providing recommendations for protection services via the web-based interface. These capabilities allow the user to conduct risk assessment and provide recommendations for protection services.

To use the information supplied by the user for the purpose of producing risk predictions, an extra layer is required. In this particular methodology, the Middleware component (Step 2) is the one responsible for carrying out the actual execution of this task. After the Request Processor has been given the client's request, it will immediately begin processing the request and will then send the data on to the Profile Evaluator. This latter component is accountable for interacting with the Machine Learning models, evaluating the prediction conclusion, and enabling a connection with MENTOR, provided that specific requirements are satisfied (Step 6).

In order to make an accurate estimate of the level of risk involved, a request is sent to the Risk Classifier. A prediction tool known as the Risk Classifier has been included into the ML Classifier Layer (Step 3) of the model. Its major responsibility is to provide API access to the machine learning models that have been trained. In addition, the ML Classifier Layer remembers both the trained ML models and the Data Scalers that were used to normalize the input data and improve the accuracy of predictions. Both of these things are stored in the memory of the layer.

In the fourth step of the machine learning workflow, also known as Step 4, the training, validation, and testing of ML models take

place. These processes are often carried out by data scientists or other professionals from inside the business. To provide a brief summary, the Data Generator module is what is used to get the process of producing synthetic data started. After that, the information is processed by an individual who is specifically designated as the Data Processor, and after that, the information is used by the Model Builder to support the processes of training, validating, testing, and creating the models. The next part presents an in-depth analysis of each phase of the ML Workflow, with the appropriate amount of focus placed on the corresponding degree of detail. The interface that is offered in Step 5 includes a monitoring API that makes it possible to verify the status of the models that have been deployed, get model-specific information such as version, creation time, and accuracy, and see additional metrics about the prediction service such as request duration in seconds.

The procedure to follow while carrying out risk assessments.

Following the steps of identifying and gaining an understanding of the potential applications of machine learning in cybersecurity risk assessment, the next step involves getting started on the process of designing and developing a machine learning workflow. Flow chart representation of the supervised machine learning process can be found in Figure 4 of this thesis. This workflow, which is an essential part of the solution, is shown in the form of a flow chart. The gathering of data is the first step that is of the highest relevance. This step comes immediately after the formulation of the issue statement. During this stage, information is typically gathered from a variety of sensors or sources and then archived for later use in an analysis stage. When it comes to the evaluation of cybersecurity risks, it is fairly uncommon for businesses to either not provide any information entirely [93] or to produce inadequate reports that make it

difficult to extract major and notable results. As a way of finding a solution to this issue, a process that involves the generation of synthetic data was conceptualized and put into action.

The act of accumulating or amassing information or data.

Data that is created via the use of different algorithms with the goal of reproducing the statistical properties of the original data while guaranteeing that no identifying information about the subjects is published is referred to as synthetic data. The word "synthetic data" is the term that is used to describe this kind of data. The following criteria have been formed as the basic foundation for this research after a complete investigation and assessment of numerous cyberattacks and related contextual information of firms. This inquiry and examination were carried out in order to establish the fundamental basis for this study.

Revenue. The word "revenue" refers to the profits that are created from normal company activities, and it is often used to classify enterprises based on a measure that is applied for the purpose of measuring the magnitudes of the organizations [98].

The making of investments in computer security. In most cases, businesses have formed cybersecurity investment plans that they have put into action in order to provide an acceptable degree of protection. The aforementioned data has to be included into the process of evaluating the cybersecurity risk since it has the potential to have an effect on the likelihood of becoming the target of a cyberattack.

In this particular research, the variables that are of interest are the total number of workers and the education level of those employees. It is vital to include the number of personnel in a business and their associated degree of cybersecurity training, including basic knowledge and phishing training, as crucial contextual information when assessing

possible cyber-risks. This should be considered in tandem with the income of the organization. The measurement of the degree of employee training is divided into three stages, which are referred to as "Low," "Medium," and "High."

A look at the results of a study on cybersecurity incidents. The aforementioned characteristics are meant to indicate the total number of cyberattacks that the company has been subjected to during the course of its existence. The aforementioned includes a number of attacks, such as Distributed Denial of Service (DDoS), Ransomware, and Phishing, which have been aimed on the infrastructure of the business and have resulted in either monetary loss or damage to its reputation. The infrastructure of the entity has been the target of these attacks. Efforts that are not fruitful are also accorded the respect they deserve.

The flaws that have been identified up to this point. It is very necessary to be completely transparent about any and all infrastructure-related weaknesses that have been discovered in order to carry out an accurate and exhaustive risk assessment. The employees responsible for an organization's information technology security often have an important duty in the management of vulnerabilities. Evaluation and documentation of any possible security flaws that may already exist inside the organization's systems is normally the task of the first stage, which comes first in the process. For the purpose of vulnerability scanning, a wide variety of comprehensive tools, such as Nmap, Metasploit, and OWASP, are employed. At the moment, the total count of discovered vulnerabilities is calculated throughout the process of synthetic creation. This is how it works.

An person who offers advise services about matters pertaining to cybersecurity from an external point of view. It is recommended that companies make use of the services of external Cybersecurity Advisors (CSAs) in order to strengthen their resistance to

cyberattacks [102]. These consultants are able to provide a hand in the processes of defending against, reacting to, and recovering from cyberattacks. In addition, it is important to note that the CSA provides a wide variety of services, which include, but are not limited to, cyber readiness, tactical communication, facilitation of collaborative efforts, partnership cultivation, evaluation of cyber risks, and provision of assistance in managing cyber incidents [102]. It is worth noting that the CSA provides all of these services. During the phase of the process known as the generation of synthetic data, a binary value will be produced. This value has the potential to take on either "Yes" or "No" as its value, the two options available to it.

Risk. The last parameter designates the qualitative risk assessment value that is obtained from the factors discussed before. The purpose of producing historical records of organizations that operate in industries that are comparable is one of the goals of the process of creating synthetic data. As a consequence of this, the value of the risk column may be derived using more traditional formal or individualized qualitative risk assessment approaches, as was covered in Section 3. The possible danger that is generated may be placed into one of three separate categories: "Low," "Medium," or "High."

It is important to notice that the probability of risk occurrence is not a random occurrence but rather a calculated result based on the qualities that are created and displayed in Table 4.1. This is significant because it means that the likelihood of risk occurrence is not a random phenomena. This is accomplished by making use of a standard mathematical formula (1). It is essential for there to be labels present within the dataset if one wishes for supervised learning to be successful. As a consequence of this, the result of the risk estimate is placed into one of these three buckets: "Low," "Medium," or "High." However, considering the fact that the final dataset would contain a

great number of entries, the process of manually labeling each item would prove to be prohibitively expensive. As a consequence of this, a mapping range was determined by basing it on the numerical value of the risk calculation. As a consequence of this, one may draw the conclusion that each risk value that has been computed has been given a label according to the range described in Equation 2.

$$risk(x) = \begin{cases} High, & \text{for } x < 0 \\ Medium, & \text{for } 0 \leq x < 1 \\ Low, & \text{for } x \geq 1 \end{cases} \quad (2)$$

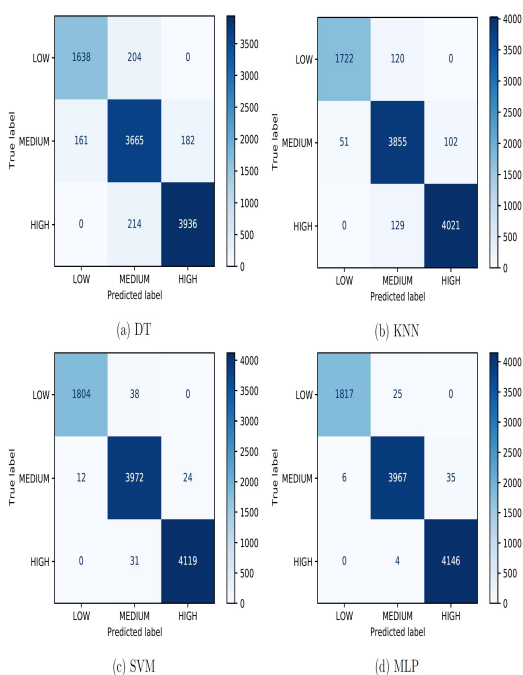


Figure 4: Confusion matrices

The number of examples that were incorrectly categorised in relation to the total number of classes that were anticipated. As can be seen in Figure 6.1, the in question prototype had a success rate that was more than 90% for each model it produced. The cells that are directly

near to the diagonal demonstrate that DT and KNN performed somewhat worse than SVM and MLP did when it came to classification accuracy.

The performance metrics that were calculated using a dataset containing 50,000 items are shown in the table below. Every model went through training and tuning procedures so that it could achieve the highest possible accuracy, minimize the risk of overfitting, and produce the best possible results. Classifiers based on Support Vector Machines (SVM) and Multi-Layer Perceptrons (MLP) were found to have accuracy levels that were equivalent to one another. Nevertheless, there is a significant gap between the two models in terms of how efficiently they can be computed. When it comes to the training phase, it is clear that the SVM model requires approximately half the amount of time that the MLP model does. This is something that can be witnessed. Grid search is a method of hyperparameter optimization that was covered in Chapter 4; the length of the training period has a major impact on the amount of time required for its calculation. The calculation time for the MLP model is more than 200 seconds due to the fact that every optimized model is subjected to a 5-fold cross-validation. In contrast, it can be seen that the DT and KNN algorithms demonstrated the lowest duration for training, with KNN displaying the swiftest calculation time for grid search at roughly 40 seconds. DT also exhibited the shortest period for training overall.

Figure 4 shows confusion matrices that may be used to produce important metrics like as precision, recall, and F1-score. These metrics can be obtained by using these matrices. The accuracy measure is the ratio of examples that were categorized by a model as belonging to a given category, and those instances do in fact belong to that category. The decision tree method accurately predicted a "Low" risk for a total of 1638 profiles out of the whole set of projected profiles (1638 + 161 + 0), as shown

in Figure 4a. This resulted in an accuracy rate of roughly 91% (1638 / 1799), given that there were a total of 1799 profiles.

In addition, the recall metric is used to determine how accurate a model is in making predictions on a particular category. In a nutshell, it refers to a model's ability to determine, within the confines of a specified dataset, each and every occurrence that falls into a certain output category. The decision tree method was able to obtain a recall rate of around 89% (i.e., 1842 profiles divided by 1638), as shown in Figure 6.1a. This rate was calculated by dividing the total number of profiles with a true label of "Low" against the number of profiles that were properly categorized. There were 204 profiles that were incorrectly classified.

3. QUALITATIVE EVALUATION

Case Study #1 - DDoS Attack

Within the scope of this research, the capability of SecRiskAI to assess the threat posed by DDoS assaults is investigated and analyzed. In order to accomplish this goal, it is important to train a machine learning model using data that is separate from the datasets that were used for the quantitative evaluation. Modifications were made to the process of producing synthetic data in order to develop a unique set of characteristics that have a direct impact on the likelihood of a company becoming the target of distributed denial of service attacks (DDoS). Following an in-depth investigation, the characteristics that serve as contextual data were determined to be those that denote the industry as well as the geographical area. Additional variables, such as workforce size and employee education, were not included in the generation phase because there was insufficient evidence to support their influence on DDoS vulnerability, as indicated by prior research. This decision was made because of the lack of evidence.

Following the qualitative evaluation that was described earlier, a dataset with 30,000 entries was produced, and the MLP was found to be an appropriate model for predicting DDoS vulnerability. This was accomplished thanks to the results of the evaluation.

Regarding the specifics of the context, it was assumed that the company that wanted to assess the DDoS vulnerability was a participant in the E-Commerce sector and was involved in the buying and selling of a variety of goods over the internet, with a major concentration on the European market. This was a presumption based on the assumption that the company wanted to analyze the DDoS vulnerability. In addition, the overall number of workers is somewhere about 10,000, and their degree of expertise in topics related to cybersecurity, which is more usually referred to as their "awareness level," was rated as "low." Figure 5 illustrates that further extensive information consist of a firm value of around 5 million United States dollars and an allocation of only 50,000 United States dollars for cybersecurity spending. The current investigation focuses on the question of how much of the budget for cybersecurity should be allotted to various types of protection services, such as those that are either proactive or reactive in nature, as well as other expenditures that aim to improve the system's resistance to DDoS assaults.

Figure 5: E-Shop contextual information

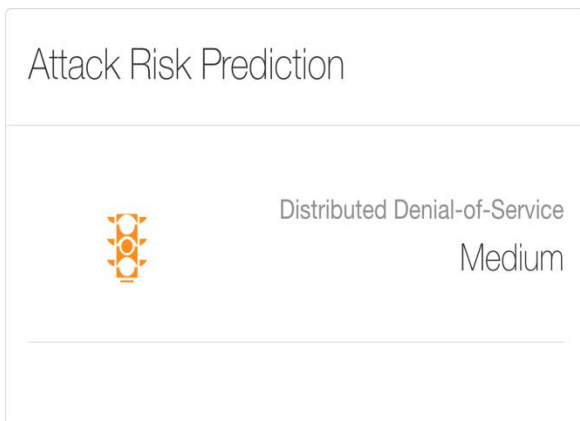


Figure 6: DDoS risk prediction

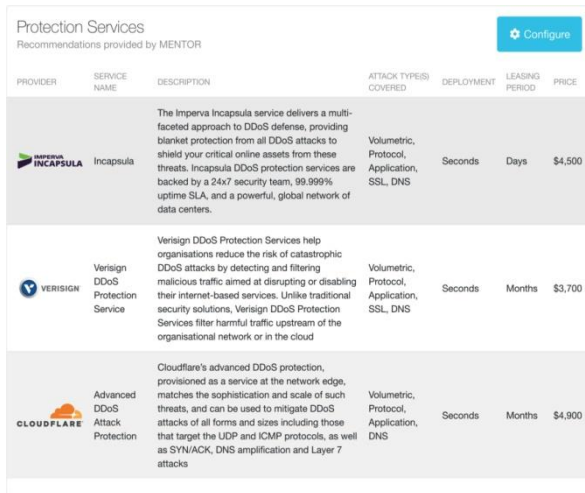
After that, the profile is subjected to an update before being sent to the backend of SecRiskAI for further analysis. The user may get access to the dashboard by employing the sidebar. The dashboard displays contextual information in a way that is easy to understand and instantly launches risk prediction. The machine learning classifier is assigned with the responsibility of producing the final forecast, while the middleware is tasked with the responsibility of processing the company's

profile. The user-friendly frontend then incorporates the answer that was provided by the prediction into the dashboard once it has been processed. The statistics that are shown in Figure 6 indicate that the specified profile has a "Medium" degree of DDoS risk. This conclusion was reached after analyzing the data".

Case Study #2 - Recommendation of Protections

Se-cRiskAI offers a seamless integration with MENTOR, a supporting tool that focuses on recommending cybersecurity protection services, in order to improve the efficiency and dependability of the risk assessment technique. This is done in order to increase the effectiveness and reliability of the risk assessment procedure. In order to provide recommendations in relation to DDoS assaults, a pre-existing integration has been developed with MENTOR. In light of the DDoS risk assessment, the primary focus of this particular case study is an investigation of the various investment opportunities available. When requesting a list of recommendations, it is the responsibility of the E-Shop to provide a set of desired parameters that are essential for the recommendation process. In the beginning, SecRiskAI will provide you with some predefined parameters, but the organization reserves the right to change these parameters as it sees fit. The dashboard, which has a panel that displays the aforementioned information, is shown in the diagram as having such a panel.

Figure 7: Protection service parameters panel






PROVIDER	SERVICE NAME	DESCRIPTION	ATTACK TYPE(S) COVERED	DEPLOYMENT	LEASING PERIOD	PRICE
	Incapsula	The Imperva Incapsula service delivers a multi-faceted approach to DDoS defenses, providing blanket protection from all DDoS attacks to shield your critical online assets from these threats. Incapsula DDoS protection services are backed by a 24x7 security team, 99.999% uptime SLA, and a powerful, global network of data centers.	Volumetric, Protocol, Application, SSL, DNS	Seconds	Days	\$4,500
	Verisign DDoS Protection Service	Verisign DDoS Protection Services help organisations reduce the risk of catastrophic DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling their internet-based services. Unlike traditional security solutions, Verisign DDoS Protection Services filter harmful traffic upstream of the organisational network or in the cloud.	Volumetric, Protocol, Application, SSL, DNS	Seconds	Months	\$3,700
	Advanced DDoS Attack Protection	Cloudflare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of such threats, and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks.	Volumetric, Protocol, Application, DNS	Seconds	Months	\$4,900

Figure 8: MENTOR's recommendations list

The protection service may be adapted to cover a variety of particular attack types, such as those designated by the firm to be Volumetric, Application, DNS, or SS-L/TLS attacks, among others. In addition, the sort of service may either be proactive, meaning that it offers protection against prospective assaults in the future, or reactive, meaning that it offers security immediately after an attack has taken place. Additionally, it is possible to specify the preferred duration for deployment, which refers to the amount of time needed for the service to become operational. Additionally, it is possible to specify the leasing period, which denotes the amount of time for which the organization is willing to lease the service under contract, along with the priority that has been assigned. When making recommendations, additional factors, such as the proportion of an organization's resources that are devoted to cybersecurity and its location in the world, are essential variables that are taken into account. When the dashboard is loaded, a process analogous to the forecasting of cyber-risk called the recommendation process for the e-shop is

immediately started with the parameters set to their default values.

4. CONCLUSIONS

The major purpose of this thesis was to plan for and carry out the creation of a tool called SecRiskAI, which is powered by machine learning and is designed to make the process of evaluating a company's cybersecurity risk easier. At first, the process for risk assessment was developed, which included many essential steps such as data collecting, data manipulation, the selection of a machine learning model, and performance evaluation. In this work, the applicability of four different machine learning algorithms—specifically, Decision Trees (DT), Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Multilayer Perceptron (MLP)—was investigated for its potential use in predicting and assessing the likelihood of cyber attacks. For the purpose of accomplishing this goal, data sets of varied sizes were generated and used throughout the training and testing phases of each machine learning model. Following the completion of testing and validation, the models were incorporated into the machine learning classifier that SecRiskAI had developed. This classifier offered a number of API endpoints, the majority of which were used by the graphical user interface (GUI).

The proof-of-concept that has been completed is capable of assessing the potential hazard only for a subset of well known cyber assaults. More specifically, it can evaluate the potential hazard for distributed denial-of-service (DDoS) and phishing attacks. In order for the prototype to be able to accomplish this goal, it need a unique collection of attributes, which is more frequently referred to as a profile or contextual data. SecRiskAI makes use of this kind of data to make predictions on the likelihood of being targeted by phishing or distributed denial of service attacks. In addition, the current prototype makes it

possible to integrate with MENTOR, which results in the provision of a list of protective services that are proposed to the user based on the user's profile and the calculated level of cyber-risk. In addition, the MENTOR integration was purposefully designed to be totally modifiable. This enables the user to adjust the integration and give different priority levels to different profile characteristics, which in turn kicks off a new mechanism for making recommendations.

Prospective research comprises the investigation and analysis of risk variables that may or may not play a role in the creation of machine learning models that are unique to cyberattacks. This kind of study is also referred to as exploratory research. These models have the capacity and specialty to evaluate the danger posed by various classes of cyberattacks, making it possible to conduct a phase of cybersecurity risk assessment that is more thorough. When applied to real-world datasets, the machine learning models that are now included into SecRiskAI need to be evaluated on their performance and effectiveness, and this evaluation requires more empirical research to be conducted. It is recommended that in the course of future research activities, consideration be given to examining the practicability of getting prediction feedback in order to determine whether or not it may improve the efficiency and comprehensiveness of machine learning models. Future research endeavors should also investigate the aspect of ongoing risk surveillance. This is the process by which crucial risk indicators are consistently gathered and leveraged for automated and uninterrupted evaluations of cybersecurity risks. This is done with the intention of approximating the probability of unforeseeable cyber hazards.

REFERENCES:

- [1] Louis Columbus: The Best Cybersecurity Predictions For 2021 Roundup. <https://www.forbes.com/sites/louiscolumbus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/>, (Last accessed April 2021).
- [2] JonOltsik: Cyber risk management continues to grow more difficult. <https://www.csoonline.com/article/3324363/cyber-risk-management-continues-to-grow-more-difficult.html>, (Last accessed April 2021).
- [3] Thomas Poppensieker: A new posture for cybersecurity in a networked world. <https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world>, (Last accessed April 2021).
- [4] IBM Security: Cost of a Data Breach Report. <https://www.ibm.com/downloads/cas/RDEQK07R>, (Last accessed April 2021).
- [5] ISO: Risk management - Guidelines. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>, (Last accessed April 2021).
- [6] The OpenGroup: The TOGAF Standard. <https://publications.opengroup.org/c182>, (Last accessed April 2021).
- [7] National Institute of Standards and Technology (NIST): SP800-30. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>, (Last accessed April 2021).
- [8] Salvatore Marco Pappalardo, Marcin Niemiec, Maya Bozhilova, Nikolai Stoianov, Andrzej Dziech, Burkhard

- Stiller: Multi-Sector Assessment Framework - A New Approach to Analyse Cybersecurity Challenges and Opportunities, Springer, CCIS, pp. 1-15.
- [9] Deloitte.:Why artificial intelligence is a game changer for risk management. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-ai-risk-powers-performance.pdf>, (Last accessed April 2021).
- [10] Maxwell W. Libbrecht, William S. Noble: Machine learning applications in genetics and genomics, Nature Reviews Genetics volume 16, pp. 321-332, 2015.
- [11] Konstantina Kourou, Themis P.Exarchos, Konstantinos P. Exarchos, Michalis V. Karamouzis, Dimitrios I. Fotiadis: Machine learning applications in cancer prognosis and prediction, Computational and Structural Biotechnology Journal Volume 13, 2015, pp 8-17.
- [12] B. Rodrigues, M. F. Franco, G. Paranghi, B. Stiller: SEconomy: A Framework for the Economic Assessment of Cybersecurity; 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019), Springer, Leeds, UK, pp. 1-9.
- [13] M. Franco, B. Rodrigues, B. Stiller: MENTOR: The Design and Evaluation of a Protection Services Recommender System; International Conference on Network and Service Management, Halifax, Canada, 2019, pp. 1-7.
- [14] M. Franco, E. Sula, B. Rodrigues, E. Scheid, B. Stiller: ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections; International Conference on Economics of Grids, Clouds, Software and Services (GECON 2020), Izola, Slovenia, September 2020, pp 1-12.
- [15] P. Radanliev: Artificial Intelligence and Cyber Risk Super-Forecasting; University of Oxford, Department of Engineering Science, Pre-Print, March 2020.