Mesopotamian journal of Cybersecurity
Vol. 2022, **pp**. 28–37
DOI: https://doi.org/10.58496/MJCS/2022/004; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

Introduction to The Data Mining Techniques in Cybersecurity *

Israa Ezzat Salem[1,*], Maad M. Mijwil[1], Alaa Wagih Abdulqader[1], Marwa M. Ismaeel[1], Anmar Alkhazraji[2,1], Anas M. Zein Alaabdin [3]

[1] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Iraq*

[2] *Computer Engineering Department, Karabuk University, Karabuk, Turkey*

[3] *Public Health and Family Medicine Department, Faculty of Medicine, Jordan University of Science and Technology, Irbid, Jordan*

ARTICLE INFO

Article History

Received 12 March 2022
Accepted 20 May 2022
Published 30 May 2022

Keywords

Data mining

Cybersecurity

Artificial intelligence

Internet

Viruses

ABSTRACT

As a result of the evolution of the Internet and the massive amount of data that is transmitted every second, as well as the methods for protecting and preserving it and distinguishing those who are authorized to view it, the role of cyber security has evolved to provide the best protection for information over the network. In this paper, the researcher discusses the role of data mining methods in cyber security. Data mining has several uses in security, including national security (for example, surveillance) and cyber security (e.g., virus detection). Attacks against buildings and the destruction of key infrastructure, such as power grids and telecommunications networks, are examples of national security concerns. Cybersecurity is concerned with safeguarding computer and network systems from harmful malware such as Trojan horses and viruses. In addition, data mining is being used to deliver solutions such as intrusion detection and auditing.

1. INTRODUCTION

As a result of the proliferation of digitalization, enormous volumes of data are being transferred from one network to another [1]. The attacker or intruder uses a variety of methods to monitor the network in order to get crucial information. This is done in order to gather data. By analyzing your databases and security logs using data mining methods, you may be able to detect malware, system and network intrusions, insider attacks, and a wide range of other security issues. Some methods are even capable of accurately forecasting attacks and locating risks that have not yet been discovered. Data mining gives you the ability to quickly evaluate enormous datasets and find hidden patterns, which is essential for designing an effective anti-malware solution that is able to detect threats that have not been found before. The quality of the data that is used in the data mining procedures will ultimately determine the results that are produced. Gathering information patterns is one of the functions of intrusion detection, after which an effort is made to assess whether or not the pattern is harmful. Anomaly detection and abuse detection are the two categories that fall under the umbrella of intrusion detection. Anomaly is in charge of monitoring how the data is behaving, while Misuse analyzes how the data compares to the attacked pattern that is stored in the database. Both of these functions are part of the data integrity module [2]. IDS systems that are built on data mining have the ability to discover these user-interesting data in a time-efficient manner and to predict the consequences that may be employed in the future. Both the information technology industry and society as a whole have shown a lot of interest in data mining, often known as the finding of knowledge in databases. Data mining is a technique that has been used to derive useful information from vast quantities of unstructured, inconsistent, and ever-changing data [3]. In Figure 1, you can see the IDS architecture in its entirety. It is strategically located in the middle of the network so that it can collect all of the incoming packets that are sent across it. After the data have been gathered, they are sent to be preprocessed so that the noise can be removed, and unnecessary or missing characteristics may be substituted. After that, the data that have been preprocessed are examined and categorized according to the severity measures they include. If the record is normal, there is no need for any more adjustments to be made; otherwise, it will be submitted for report creation in order to trigger alarms. Alarms are triggered depending on the state of the data in order to motivate the administrator to find a solution to the issue in advance. The purpose of the attack is to enable the classification of the network's data. As

*Corresponding author. Email: israa.ezzat@baghdadcollege.edu.iq soon as the transmission starts, all of the actions that came before it are carried out once again [4][5]. The major focus of this study will be placed on the application of data mining methods to the challenge of ensuring the safety of digital networks. It is essential to have an awareness of the many kinds of dangers that might be presented to the computer network of a country in order to have an understanding of the approach that will be used to protect the computers and network of the nation. The structure of the intrusion detection system is shown in its entirety in Figure 1. Software intrusion detection is the process of detecting intrusions using various methods. More specifically, it refers to the collection of various user activity behavior data both inside and outside the system. Additionally, it performs a comprehensive analysis of various internal and external user activity data to discover and identify abnormal system behaviors [6].

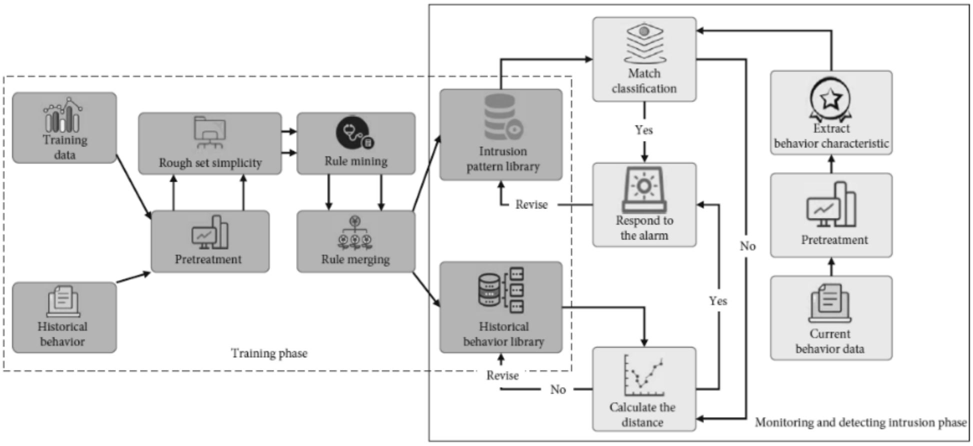

Fig. 1. The mechanism of data mining technology in intrusion detection [7]

The following are some uses of data mining that may be used for the identification of intrusions:

- The purpose of intrusion detection is to find holes or lapses in the security of information systems. A passive approach to security, intrusion detection involves the monitoring of information systems and the generation of alerts in the event that a security breach is discovered.
- The Risk Assessment and Fraud sector employ the same concept of data mining in order to, among other things, discover improper or unusual activities.

The use of data mining makes it possible to retain customers by enabling the identification of patterns of customer churn and the prediction of future customer churn [8]. The following is a list of the several applications that data mining technology may have for the purpose of intrusion detection.

- Using data mining methods to develop a new model for intrusion detection systems: The data mining approach used by the IDS model achieves a higher rate of efficiency with less incidence of false positives. The techniques of data mining may be used to locate signatures in addition to abnormalities. In signature-based detection, training data is evaluated to determine if it is "normal" or a "intrusion." It is possible to build a classifier in order to identify known breaches in security. In this field of research, several software applications, such as clarifying algorithms, association rule mining, and cost-sensitive modeling, have been investigated. The creation of models of usual behavior and the automated discovery of large deviations from these models are the two main functions of anomaly-based detection. Software for clustering data, software for analyzing outliers in the data, class algorithms, and statistical methodology are all examples of methods. The approaches that are applied need to be effective and scalable, in addition to being able to deal with enormous volumes of data that are high-dimensional and come from a variety of community sources.
- Stream data analysis: Stream data analysis includes evaluating data in real time, while data mining is often used on static data due to the complex computations and lengthy processing periods involved in the process. It is becoming more important to do intrusion detection when the records stream context is being used. This is due to the dynamic nature of incursions and efforts at being malevolent. In addition, an event could seem innocuous when seen as a stand-alone occurrence, but it might be regarded malicious when viewed as part of a pattern of actions. As a consequence of this, it is of the utmost importance to investigate the activity sequences that are most commonly seen together, as well as to discover sequential patterns and outliers. In order to recognize shifting clusters and construct dynamic class models in record streams, which are both necessary in order to identify intrusions in real time, other data mining approaches are needed as well.

- Distributed data mining: This technique is used to investigate random data that is inherently dispersed throughout various databases, making it challenging to integrate data processing. The source of an intrusion may be anywhere, and it can go anywhere it wants to go. Several distinct locations are possible starting points for an intrusion. It is feasible to use methods for distributed data mining in order to study community data that has been obtained from a number of different network locations in order to discover assaults that have propagated.
- Instruments for visualizing data: The user is able to acquire a better visual understanding of the data by using these tools, which portray the data in the form of graphs. These tools are used in the process of visualization creation. In addition to that, these instruments are used in the process of analyzing any unique patterns that have been identified. There is a possibility that one of the capabilities supplied by these technologies is the ability to investigate correlations, discriminative patterns, clusters, and outliers. Structures for intrusion detection are required to provide a graphical user interface that enables security analysts to pose inquiries about network data or the results of intrusion detection.

2. LITERATURE SURVEY

Information security has been an essential factor in determining the success or failure of future advancement from the beginning of time. In the past, information was gathered manually, and there was limited access to efficient means of preserving this data. Because of the rapid advancement of technology, there has been a considerable growth in the number of techniques for preserving information; nevertheless, security is also becoming a serious problem as a result of the growing number of security risks. Concerns of this kind about information security may arise on a desktop computer, in an office environment, on a network, or in the cloud. According to the findings of the literature review, data mining is an essential component in the process of addressing challenges related to information security. In [9] provides a description of the soft computing framework for data mining. This page also explores several soft computing approaches, such as fuzzy logic and neural networks. The authors of [10] examines the development of data mining as well as the many fields in which it may be used. Data mining offers a variety of techniques that may be used to help in the identification and avoidance of potential security risks [11-13]. The authors of the study [14] provides a review of a number of data mining methods for intrusion detection, as well as a synopsis of the many types of intrusion attacks, including network and host-based intrusions. There is a method of There is a kind of intrusion detection that is often referred to as anomaly detection, and it has received a significant amount of attention [15]. The examination of network intrusion technologies is now a topic that is getting a lot of interest, and one of the topics being discussed is the use of data mining and machine learning methodologies to the research of these technologies. Improving the effectiveness of the detection of intrusions into computer networks is a challenging problem. rates based on a single defining property or detecting model. The performance of the given model is verified using a publicly available database. The writers of the article [16] wants to bring attention to the possible problems with an individual's privacy that might arise as a direct consequence of data mining. Niranjan et article's [17] have an author whose mission is to study the importance of data mining techniques in the process of achieving security. The scope of this study is limited to a few applications, including phishing website classification, privacy preserving data mining (PPDM), Intrusion detection system (IDS), Anomaly/Outlier Detection, and code injection and reuse attack mitigation. In [18] presents a one-of-a-kind anomaly detection approach that can be utilized to detect previously undiscovered network assaults by detecting the substantially relevant attack aspects. This method is described as being able to be utilized to detect previously undiscovered network assaults. When operators of computer networks are aware of these factors, their situational awareness will improve, which will lead to an increase in the efficiency of computer network defense. The following are some contributions that have been made as a result of this effort. To begin, the novel combination of methods that were utilized in this research, namely k-means clustering, Nave Bayes, Kruskal-Wallis, and C4.5, makes it possible for cyber attacks to be targeted with a high degree of accuracy within an environment that is characterized by congestion and conflict in the cyber network. An intrusion detection system was reported by [19]. This system used J48 decision tree data mining methods and an Oak Ridge National Laboratories (ORNL) data set. According to the findings of this study, decision trees are superior to other controlled techniques in terms of their level of precision.

3. INFORMATION SECURITY

The process of protecting data against unauthorized access, disclosure, interruption, modification, or destruction is referred to as information security, which is sometimes referred to by its acronym, Info-Sec. Computer and communication systems are notoriously vulnerable to intrusions of privacy and violations of data security. The majority of modern organizations allocate a significant portion of their budgets to the protection and privacy of their networks. People are becoming increasingly oriented toward regular use of information technology, which has led to increased use of online resources. This increased use of online resources has resulted in the birth of a great number of security risks to these resources. People are becoming increasingly oriented toward regular use of information technology. The three primary tenets of information security, namely confidentiality, integrity, and availability, are shown graphically in Figure 2. The information security program must be designed in such a way that each individual component incorporates at least one of these ideas. When they cooperate, this group is sometimes referred as the CIA Triad.

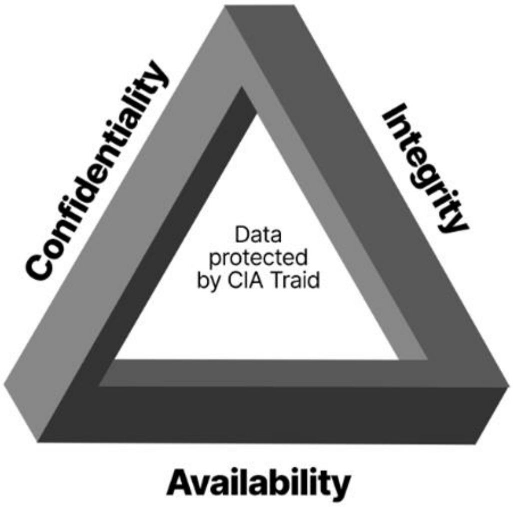

Fig. 2. Attribute of Information Security [20].

3.1 Confidentiality

Safeguards for confidentiality are measures taken with the intention of preventing the unauthorized distribution of information. The purpose of the confidentiality principle is to ensure that personal information is protected from public view and that it is available to only those individuals who are in possession of the information or who need it to carry out their duties within the organization. Integrity of data requires protection against alterations made without authorization (additions, removals, updates, and so on). The integrity principle ensures that the data is correct and reliable, and that it is not updated in an incorrect manner, whether by accident or on purpose. It also ensures that the data is not altered in an incorrect manner.

3.2 Availability

The protection of a system's capacity to render all of its software systems and data completely available at any moment that a user makes a request for it is what is meant by the word "availability" (or at a specified time). The purpose of making the technical infrastructure, applications, and data accessible whenever they are required for a process carried out by an organization or for the customers of that business is known as the objective of availability.

4. CYBERSECURITY

The term "cybersecurity" refers to a set of guidelines and technologies that together are intended to protect our computer systems, networks, and data against unauthorized access, attacks, and disruptions [21]. They make an effort to protect the confidentiality, integrity, and availability of information and information management systems by using a variety of cyber defensive measures. Cyber security experts and researchers from institutions, commercial enterprises, academic institutions, and government organizations have participated in a growing collaborative effort to exploit and create a range of cyber defensive systems to protect cyber infrastructure from potential hostile threats. This effort has led to the development of a variety of cyber defensive systems. Figure 3: An established method of computer network protection the term "cyber security systems" together refers to both network security systems and host security systems. Each of them is geared up with an intrusion detection system, antivirus software, and a firewall (IDS). The second line of defense in a computer network is made up of reactive security solutions such as intrusion detection systems (IDSs). IDSs analyze the extent of damage caused by intrusions, track down hackers, and prevent future attacks by utilizing information gleaned from log files and activity on the network to detect and locate instances of intrusion. The process of examining data from a particular source and assembling that input into useful information is referred to as "data mining," but it is also known by its acronym, KDD, which stands for "knowledge discovery." In terms of protecting information online Mining methods are being used to data in order to identify potentially hazardous situations [22].

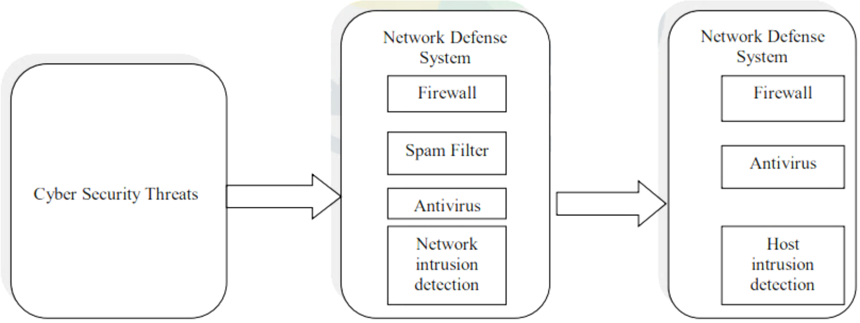

Fig. 3. A traditional cybersecurity mechanism [22].

There are a few straightforward tools that may be used to detect cyberattacks, including the following: Information may be protected using cryptography by having its data converted into a format that is not readable (cipher text). Those individuals who are in possession of the hidden key are the only ones who can interpret this message. The process of reviewing data collected from networks and information systems in order to determine whether or not a security breach or security violation has occurred is referred to as intrusion detection. Testing a network or information system by penetrating it is a method of assessment in which evaluators search for vulnerabilities in the target system. Today, people and families, along with organizations, governments, educational institutions, and our enterprises, see cybersecurity as a crucial component. This view is shared across all of these other sectors as well. It is essential for parents and families to take measures to shield their children and family members from the dangers posed by the internet. It is essential that we protect our financial information, which might have an effect on our own personal financial condition. This is important in the context of maintaining our financial safety. Internet usage is very crucial and beneficial for educators, students, and staff members at educational institutions since it has opened up many new opportunities for learning while also providing a number of different dangers to students and staff members online. Users of the Internet need to educate themselves on how to defend themselves against identity theft and fraud committed online. A decrease in the number of vulnerabilities and an increase in online safety may be achieved by proper behavior and adequate system security. The issues that affect small and medium-sized enterprises are quite similar. Users of the Internet need to educate themselves on how to defend themselves against identity theft and fraud committed online. A decrease in the number of vulnerabilities and an increase in online safety may be achieved by proper behavior and adequate system security. Small and medium-sized firms suffer a range of security challenges due to limited resources and insufficient cyber security knowledge. These challenges may be broken down into many categories. The rapid growth of technology is not only generating and making cyber security more difficult since we do not supply permanent remedies to the situation at hand, but it is also providing these answers. In spite of the fact that we are actively engaged in combat and providing a large number of frameworks or technologies to secure our network and information, none of them provide any protection beyond the immediate term. Having a more in-depth understanding of security and appropriate approaches, on the other hand, may help us secure intellectual property and trade secrets, therefore minimizing the potential damage to our finances and reputation. Because of the large volumes of data and private information that are kept in digital form by central, state, and local governments, these levels of government are excellent targets for cyber assaults. The majority of the time, governments are forced to deal with difficulties as a result of poor infrastructure, a lack of understanding, and an insufficient budget. It is essential for governmental organizations to provide reliable services to the general public, to keep lines of communication open with the people they serve, and to protect sensitive information [25].

Information security is distinct from cybersecurity in both its scope and its intended purpose. The two terms are commonly interchanged; nevertheless, information security is a broader category than cybersecurity, which is a subclass of information security. Examples of information security include things like endpoint security, data encryption, and network security. Physical security is another example. In addition to this, it is intricately connected to information assurance, which protects data from threats such as natural disasters and disruptions in server availability. The primary focus of cyber security is on the potential risks posed by new technology, as well as the strategies and tools that may be used to eliminate or reduce such risks. Another issue that is connected to this one is data security, which focuses on protecting an organization's data from being maliciously or unintentionally disclosed to third parties who are not allowed to see it.

5. DATA MINING

First things first: let's talk about what data mining is before we get into how it might be used in the context of cyber security. Data mining boils down to an identification of patterns at its core. Data miners are experts in using specialized technologies to sift through enormous data sets in search of patterns of behavior, both typical and unusual. After mining the data, the information may be used to foresee future trends, enabling companies to make proactive, knowledge-based choices based on large data sets. These decisions can be derived from the information. Depending on the specific information that users are looking for, software programs that mine data for patterns and correlations in the data can identify those. This suggests that the data is only as good as the requirements placed upon it by the data miners. The process of data mining is sometimes broken down into five stages, which are as follows:

1. Businesses begin by collecting data and then loading it into data warehouses.
2. Companies may either manage and keep their data on their own internal servers or on the cloud.
3. Management teams, business analysts, and information technology professionals review the data and determine how it should be organized.
4. The application software uses the requirements of the user to determine how the data should be arranged.
5. The information is shown by the end user in a format that makes it simple to share it with others, such as graphs or tables. Figure 5 illustrates the many different data mining strategies, including [24]:

- Clustering is the challenge of recognizing groups and structures in data that are "similar" in some fashion without utilizing known structures in the data. This may be accomplished using a process known as "clustering."
- The process of classification involves generalizing an existing structure in order to adapt it to fit brand new data. For instance, software used for email may make an effort to classify an email as either legitimate or spam. Examples of regular algorithms include decision tree learning, naive bayesian classification, neural networks (soft computing), and support vector machines.
- Regression: an attempt to find the function that most accurately describes the data while making the fewest number of mistakes possible.
- Association Rule Learning investigates potential links between the different variables.

In the realm of security, data mining may serve several purposes, including those related to national security (such as surveillance) and cyber security (e.g., virus detection). Examples of things that might compromise national security include assaults on buildings and the destruction of essential infrastructure, such as power grids and communications networks. Protecting computers and other networked devices, such as servers and routers, against malicious software like viruses and Trojan horses is the focus of cyber security. In addition, intrusion detection and auditing are two examples of applications where data mining is being utilized to give solutions.

When people think about data mining, cybersecurity is often not the first thing that comes to mind. Data mining is a process that is used by businesses to convert raw data into information that has significance. Organizations are able to get a deeper understanding of their customers by using software that searches huge databases in search of recurring trends. Before being used to produce more effective marketing strategies, increase sales, reduce expenditures, or enhance customer relations, data is often mined and transformed into information that is usable. Because the quality of the data being mined is essential to the success of data mining, just as it is to the success of any other large-scale study of data, data collecting, warehousing, and computer processing are all essential components of data mining. Data mining is becoming an increasingly popular component of comprehensive cyber security solutions used by businesses. Methods of anomaly identification, for instance, might be used to uncover unexpected patterns and behaviors. The individuals responsible for the virus might be located via the use of link analysis. The many forms of cyber-attacks may be categorized with the use of classification, and then the profiles that were created can be utilized to recognize an attack when it takes place. It is possible to utilize prediction to estimate the likelihood of future attacks based on information gleaned about terrorists via electronic correspondence and telephone talks. Additionally, data mining is being used for the purpose of auditing and detecting intrusions. Establishing a protective barrier for computer systems using technologies such as firewalls, authentication tools, and virtual private networks is the time-honored method for protecting computer systems from being attacked through the internet. Nevertheless, these approaches are almost always susceptible to attack. Because of this, the creation of intrusion detection, a security technology that augments standard security measures by monitoring systems and detecting computer threats, was required. Intrusion detection is a security technology that monitors and detects computer threats. Data mining is often used in three areas: virus detection, intruder detection, and fraud detection. It is used to enhance more conventional methods to cyber security such as firewalls and authentication systems. Mining of databases may be done either descriptively or predictively, depending on the goal. Comparatively, descriptive techniques examine and organize already existing datasets, while prescriptive methods create predictions that are based on previously observed patterns.

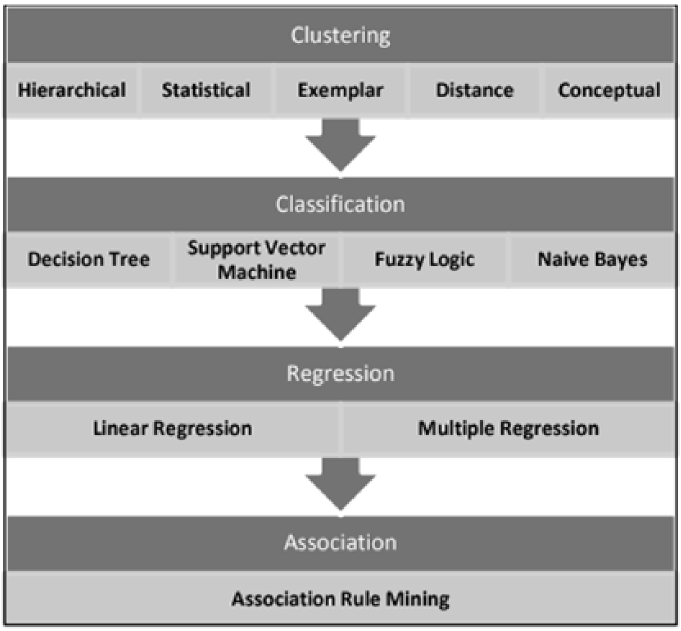

Fig. 4. Data Mining Methods [24].

When people think about data mining, cybersecurity is often not the first thing that comes to mind. Data mining is a process that is used by businesses to convert raw data into information that has significance. Organizations are able to get a deeper understanding of their customers by using software that searches huge databases in search of recurring trends. Before being used to produce more effective marketing strategies, increase sales, reduce expenditures, or enhance customer relations, data is often mined and transformed into information that is usable. Because the quality of the data being mined is essential to the success of data mining, just as it is to the success of any other large-scale study of data, data collecting, warehousing, and computer processing are all essential components of data mining. Data mining is becoming an increasingly popular component of comprehensive cyber security solutions used by businesses. Methods of anomaly identification, for instance, might be used to uncover unexpected patterns and behaviors. The individuals responsible for the virus might be located via the use of link analysis. The many forms of cyber-attacks may be categorized with the use of classification, and then the profiles that were created can be utilized to recognize an attack when it takes place. It is possible to utilize prediction to estimate the likelihood of future attacks based on information gleaned about terrorists via electronic correspondence and telephone talks. Additionally, data mining is being used for the purpose of auditing and detecting intrusions. Establishing a protective barrier for computer systems using technologies such as firewalls, authentication tools, and virtual private networks is the time-honored method for protecting computer systems from being attacked through the internet. Nevertheless, these approaches are almost always susceptible to attack. Because of this, the creation of intrusion detection, a security technology that augments standard security measures by monitoring systems and detecting computer threats, was required. Intrusion detection is a security technology that monitors and detects computer threats. Data mining is often used in three areas: virus detection, intruder detection, and fraud detection. It is used to enhance more conventional methods to cyber security such as firewalls and authentication systems. Mining of databases may be done either descriptively or predictively, depending on the goal. Comparatively, descriptive techniques examine and organize already existing datasets, while prescriptive methods create predictions that are based on previously observed patterns. Let's have a look at six crucial data mining strategies for the field of cybersecurity:

5.1 Classification

Using this method, a database model is created by segmenting a large dataset into distinct categories, concepts, and variable groups that have been specified. It is also possible to use it to evaluate new variables that have been added to the database after the model has been constructed in order to categorize the new variables. In order to achieve precise classification in real time, you will need to concentrate on supervised training of the algorithm in addition to validating the operation of the system. In the field of cybersecurity, classification is often used to identify fraudulent and spam communications.

5.2 An Examination of the Regression

These algorithms make an estimate of the changing value of one variable by comparing it to the known average values of other variables included within a dataset. You will be able to generate a relationship model in the database between the dependent variables and the independent variables if you use this strategy. Finding the causes for changes and the influence that one variable has on another may be aided by doing an analysis of variable changes and comparing those changes to dependent variables. It is standard practice to do regression analysis in order to predict trends and events, such as the possibility of cyber-attacks.

5.3 The investigation of time series

These algorithms discover and predict time-based patterns by looking at the timing of any data input changes in the database. This method, which involves mining datasets spanning several years, is highly useful for getting insights on a wide variety of different sorts of periodic activities. Time series analysis may be used to provide predictions on potential security flaws as well as assaults that may take place during a certain event, season, or even time of the day.

5.4 An Investigation into the Association Rules

One of the most widespread applications of data mining is something like this. The examination of association rules may be helpful in unearthing hidden patterns and finding plausible correlations between variables that often occur together in databases. Utilizing this method allows for the evaluation and prediction of user behavior, as well as the monitoring of network traffic and the establishment of patterns of attacks. Association rules analysis is a technique that is widely used by security personnel in order to study the behavior and cognitive processes of attackers.

5.5 Clustering

The process of clustering helps in locating data items that have similar characteristics and in comprehending the similarities and differences between variables. Clustering is analogous to classification; however, it does not allow for the immediate arrangement of variables. You will only get assistance with organizing and analyzing an existing database if you choose this technique. In contrast to classification, clustering makes it possible to make changes to models and generate subclusters without having to rewrite or otherwise modify any of the approaches or algorithms.

5.6 Summarization

The objective of this method of data mining is to compile clear and detailed explanations of datasets, classifications, and clusters. Summarization may help you better grasp the contents of your datasets as well as the consequences of the data mining process by allowing you to understand the core of the data and minimizing the need to manually search through it. It is typical practice in the field of cybersecurity to employ summarization in order to generate reports and show logs. Bear in mind that each of these methods of data mining has the potential to be improved with the help of technologies such as machine learning and artificial intelligence. You may be able to increase the accuracy of your forecasts with the assistance of these cutting-edge technologies by uncovering more hidden patterns. Nevertheless, the construction and upkeep of a cybersecurity system would almost probably become more difficult if machine learning and artificial intelligence were included into it.

6. CONCLUSIONS

Data that is trustworthy, relevant, and well-structured forms the basis of nearly every solution to a cybersecurity problem. And despite the fact that organizations produce enormous volumes of data on a daily basis, it is impossible to manually gather, analyze, and understand all of that data in order to combat cybersecurity concerns. You may detect the features of any potentially dangerous conduct with the use of data mining technologies, and you can even foresee prospective attacks using these techniques. They are very skilled in the processes of threat intelligence collection as well as the identification of malware, intrusions, fraud, and insider threats. The key benefit of bolstering your security using data mining is that it gives you the opportunity to identify unknown as well as previously recognized dangers.

Funding

None

Conflicts Of Interest

Authors declare no conflicts of interest.

Acknowledgment

Authors would like to thank the anonymous reviewers for their efforts.

References

[1] K. Aggarwal, M. M. Mijwil, AH. Al-Mistarehi, S. Alomari, M. Gök, A. M. Alaabdin, and S. H. Abdulrhman, "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," Iraqi Journal for Computer Science and Mathematics, vol. 3, no. 1, pp. 115-123, Jan. 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[2] K. L. Neela and V. Kavitha, "An Improved RSA Technique with Efficient Data Integrity Verification for Outsourcing Database in Cloud," Wireless Personal Communications, vol. 123, pp. 2431-2448, Jan. 2022. https://doi.org/10.1007/s11277-021-09248-8

[3] R. Parmar, D. Patel, N. Panchal, U. Chauhan, and J. Bhatia, "18 - 5G-enabled deep learning-based framework for healthcare mining: State of the art and challenges," in Blockchain Applications for Healthcare Informatics, 2022, pp. 401-420. https://doi.org/10.1016/B978-0-323-90615-9.00016-5

[4] G. V. Nadiammai and M. Hemalatha, "Effective approach toward Intrusion Detection System using data mining techniques," Egyptian Informatics Journal, vol. 15, no. 1, pp. 37-50, Mar. 2014. https://doi.org/10.1016/j.eij.2013.10.003

[5] I. E. Salem, M. M. Mijwil, A. W. Abdulqader, and M. M. Ismaeel, "Flight-Schedule using Dijkstra's Algorithm with Comparison of Routes Finding," International Journal of Electrical and Computer Engineering, vol. 12, no. 2, pp. 1675-1682, Apr. 2022. http://doi.org/10.11591/ijece.v12i2.pp1675-1682

[6] G. P. Bombeccari, V. Candotto, A. B. Giannì, F. Carinci, and F. Spadari, "Accuracy of the Cone Beam Computed Tomography in the Detection of Bone Invasion in Patients with Oral Cancer: A Systematic Review," Eurasian Journal of Medicine, vol. 51, no. 3, pp. 298-306, Oct. 2019. https://doi.org/10.5152/eurasianjmed.2019.18101

[7] A. Kumra, W. Jeberson, and K. Jeberson, "Intrusion Detection System Based on Data Mining Techniques," Oriental Journal of Computer Science and Technology, vol. 10, no. 2, pp. 491-496, Jun. 2017. http://dx.doi.org/10.13005/ojcst/10.02.33

[8] S. Mitra, S. K. Pal, and P. Mitra, "Data mining in soft computing framework: a survey," IEEE Transactions on Neural Networks, vol. 13, no. 1, pp. 3-14, Jan. 2002. https://doi.org/10.1109/72.977258

[9] D. Kumar and D. Bhardwaj, "Rise of Data Mining: Current and Future Application Areas," International Journal of Computer Science Issues, vol. 8, no. 5, pp. 256-260, Sep. 2011.

[10] J. Kong, C. Yang, J. Wang, X. Wang, M. Zuo, et al., "Deep-Stacking Network Approach by Multisource Data Mining for Hazardous Risk Identification in IoT-Based Intelligent Food Management Systems," Computational Intelligence and Neuroscience, vol. 2021, no. 1194565, pp. 1-16, Nov. 2021. https://doi.org/10.1155/2021/1194565

[11] A. Dogan and D. Birant, "Machine learning and data mining in manufacturing," Expert Systems with Applications, vol. 166, pp. 114060, Mar. 2021. https://doi.org/10.1016/j.eswa.2020.114060

[12] K. Patond and P. Deshmukh, "Survey on Data Mining Techniques for Intrusion Detection System," International Journal of Research Studies in Science, Engineering and Technology, vol. 1, no. 1, pp. 93-97, Apr. 2014.

[13] J. F. Nieves and Y. C. Jiao, "Data clustering for anomaly detection in network intrusion detection," Research Alliance in Math and Science, vol. 1, pp. 1-2, Aug. 2009.

[14] N. Chakraborty, Y. Mishra, and P. Chakraborty, "Data Security and Privacy of Individuals in Data Mining: A Critical Analysis of Data Mining in India," Medico Legal Update, vol. 20, no. 4, pp. 383–387, Nov. 2020.

[15] A. Niranjan, A. Nitish, and P. D. Shenoy, "Security in Data Mining- A Comprehensive Survey," GJCST-C Software and Data Engineering, vol. 16, no. c5, pp. 51-72, 2016.

[16] A. Surana and S. Gupta, "An Intrusion Detection Model for Detecting Type of Attack Using Data Mining," International Journal of Science and Research (IJSR), vol. 3, no. 5, pp. 1496-1500, May 2014.

[17] M. Gupta, J. Shriwas, and S. Farzana, "Intrusion Detection Using Decision Tree Based Data Mining Technique," International Journal for Research in Applied Science & Engineering Technology, vol. 4, no. 7, pp. 24-28, Jul. 2016.

[18] "Information Security: The Ultimate Guide," Imperva. [Online]. Available: https://www.imperva.com/learn/data-security/information-security-infosec/

[19] M. M. Mijwil, R. Doshi, K. K. Hiran, AH. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," Mesopotamian journal of cybersecurity, vol. 2022, pp. 1-4, 2022.

[20] A. Mucherino, P. Papajorgji, and P. M. Pardalos, "A survey of data mining techniques applied to agriculture," Operational Research, vol. 9, pp. 121–140, Jun. 2009. https://doi.org/10.1007/s12351-009-0054-6

[21] K. P. Barabde and V. Y. Gaud, "A Survey of Data Mining Techniques for Cyber Security," Journal of Emerging Technologies and Innovative Research, vol. 6, no. 5, pp. 360-364, May 2019.

[22] P. Aggarwal and M. M. Chaturvedi, "Application of Data Mining Techniques for Information Security in a Cloud: A Survey," International Journal of Computer Applications, vol. 80, no. 13, pp. 11-17, Oct. 2013.