International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 3, May-June 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Detection of Password-Based Attacks Using Machine Learning Techniques

Michael Osei Boateng*, Dr. Tathagata Bhattacharya**, Jaya Sai Manindhar Allam***

* Department of Computer Information Systems and Cybersecurity,
Auburn University at Montgomery, Montgomery, Alabama, USA.
moseiboateng100@gmail.com/ moseiboa@aum.edu

**Department of Computer Information Systems and Cybersecurity,
Auburn University at Montgomery, Montgomery, Alabama, USA.
tbhatta1@aum.edu
***Department of Computer Information Systems and Cybersecurity,
Auburn University at Montgomery, Montgomery, Alabama, USA.
jallam@aum.edu

Corresponding Author: Michael Osei Boateng
Email: moseiboateng100@gmail.com

Abstract

With the increasing number of accounts, security threats are increasing significantly in the past decades. Different types of attacks possess different types of threats to accounts and passwords. This paper reviews the detection of password-based attacks on different networks and various parameters on the detection probability and types of attacks in password-based systems. we created a confusion matrix of positive and negative detection. Efforts are made to restrict the crime however intruders are also have been advanced in strategizing.

Keywords-Password attacks, cybersecurity, machine learning, SVM, intrusion detection.

1. INTRODUCTION

In the general concept of people attacking Password based accounts systems, the immediate remedy that comes to mind in resolving these daily occurring menace in the field of Technology i.e., Password attacking systems has to do with the new means of using accurate detective tools or mechanisms for a user's safety. It is in the scope of a user's safety because it will prevent malicious penetration by another attacker in the accounting system.

The definition of Password is widely shown you different research scholars in computer sciences. A password is a secret word or string of characters that is used for authorization to provide identity or gain access to a resource [1]. Passwords today as you and I will agree, as you and I will agree, have come to play a most significant role in our daily life activities like computing applications like windows login accounts, internet services, and mobile phone authentications. The major objective of using a password is to restrict unauthorized users to access a system [2]. Today there are many attacks on many systems which are related to the password. Social networks on the hand have come to involve people from the entire world, of any age, and with any kind of education. Though it has to help helped in increasing computer usage among the very few that showed interest some years ago. Computer social networking platforms have become as susceptible to different types of attacks targeting different components conducted from different domains, using techniques [3]. Even though the topic under discussion is two folds, password attacks, and the detection mechanisms by employing authentication techniques and measures when there is an attempt to Toto new passwords in the account systems more like the brute forcing attacks [4]. A vast number of different verification techniques have been proposed and according to rich sources, password-based methods remain their predominant method for this case. Sophisticated methods are a clear indication that techniques are not fully coping with the demands set by computer security authorities [5].

To highlight the paper, inject attacks as a type of attack have been known as one of the most common threats to the security of database-driven applications and for that outcome, preventive defensive coding practices have offered education, but it is very difficult as some experts have perceived [6]. Applications implemented as micro-services also have larger surface areas, making them more prone to cyber-attacks. The modern operating system provides performance counters that are temper-resistant and can be used to track the run-time behavior of applications by intruders [7].

In addition to the different password attack cases, Texts passwords are also the common land in widely used authentication mechanisms on the internet and other platforms today. While users are responsible create password applications, application developers are creating codes to store passwords securely [8]. Recent studies in papers reveal that developers use to employ insecure password storage practices and have general misconceptions regarding secured password storage. Therefore, it has become important to promptly detect security issues relating to password storage before the application text is deployed. Our research paper also focuses on. The detection approach

made us look at a few points of discussion and we reviewed that; in a detection system many have suggested tools for detection. The One-type Password (OTP) and the Facial check were explained to have been used most in computing areas such as banks and it has become so important that it has prevented unauthorized users. The OTP has a predefined session of validity; today it is believed that it has become very difficult for hackers. It is described to be not vulnerable [9].

Other cyber research scholars have juxtaposed that, to defend a password there must be a proposed of some considerable web authenticating of this password and therefore a use authenticating protocol called S-Pass must be employed to prevent the attacks. The S-pass is to prevent users from typing memorized passwords into kiosks [10].
The detail of our research case study is subdivided into the various sub-topics discussed and analyzed below.

1.1 PASSWORD ATTACKS

Password Attack has become one most common attack in daily accounts activity. Password attack encompasses the act in which a hacker tries or maneuver to steal one's account holder's security Information for Data breaching or Data collection.

- It is Conjected that every 11 seconds a business falls victim to ransomware.
- About 20% of social media accounts are hacked.
- Over 80% of data breaches are due to poor password security.

When the introducer gains access to the User account. Introduce able to install malware (or) end doors which helps Keep an observation of user accounts which makes users' accounts more vulnerable. The detection System is a Monitoring device. It detects Suspicious and unauthorized activities. The system gets alerted whenever an attack is detected. The next recent requirement under the Project Group decided to use the Qualitative and Quantitative approach by gathering data through research. Secondary Sources such as research papers would be consulted. By Completing this research, we created a visualization of prediction on password-based attacks.

This Research explains the types of password-based attacks and designing a Security Mechanism Which helps to detect Suspicious activities by information and observing the case studies.

1.1.2 TYPES OF PASSWORD ATTACKS

Password attacks are one of the most important issues we face today. The accounts operation system has come to record multiple numbers of password attacks inland during our research case study, although there are different types of password attacks. In this research, we are prioritizing three types of attacks. They are Phishing attack attacks, Man in middle attacks, and Brute-force attacks.

1.1.2.1 PHISHING ATTACKS

This type of attack is when a hacker sends some sought fake email which that makes the user click if the user clicks on the email the malware in the phishing mail makes the system freeze and steals user credentials like credit card numbers and the password of the user account. Which leads dot devastating results.

1.1.2.2 MAN IN THE MIDDLE ATTACK

This type of intruder sits between two networks and deciphers communication like passwords and data. Attackers establish the connection between the user systems.

1.1.2.3 BRUTE FORCE ATTACK

This type of attack is more like a trial-and-error approach. The hacker enters entered different kinds of multiple passwords through guessing to help him open the account correctly. In this case, if you happen to have a short base password your account information would be stolen.

1.2 SECURITY ATTACKS AUTHENTICATION

To develop a secure system, we have continued competition in devising new ways to attack the security of a system accountant i.e., why this section of our paper reviewed refers to the attackers as "intruders", intruders in the sense that the intruder would only have that bolder decision to break the system in accounts, companies, or organizational management account.

In as there is a continuous occurrence of password attacks in individuals and organizational management account systems, the effort has been laid by multiple expertise in devising software tools to resist and prevent the so-called "intruders" from entering into people's accounts, hence they have been given the accolades "white hat hackers", according to Morrison and Thompson

So, for this reason, it has become important in our paper to present the history of passwords in our definition rather than simply talking about password security attacks and their detection mechanism. And the underlying goal of passwords, for example, is that entities who want to use password-based attacks all their users to have passwords to gain a high degree of security against penetration of the system account by unauthorized users.

1.3 PASSWORD-BASED THREAT DETECTION MECHANISM

Threat detection is the process of study studying a security ecosystem from top to bottom to find any malicious behavior that might put at risk the network. If a threat is identified, mitigating measures must be taken to effectively neutralize it before it can take advantage of any existing vulnerabilities. Systems penetration in an attack scenario that any organization would not wish on themselves, so most businesses organization protect their data will employ

knowledgeable personnel and cutting-edge tools to create a protective wall against any possible intruder.

Different types of detection mechanisms exist. These vary according to the type of system in operation, the levels of security needed as per the sensitivity of the data or information to be protected, and depending on the capability of implementing certain mechanisms. Threat detection falls under four classifications or categories. These are Threat Behavior, Configuration, Indicator, and Modeling. Within the mentioned categories we have various mechanisms, which an organization can apply in threat detection.

2. LITERATURE REVIEW

We will review several scholarly words on password attacks and detection mechanisms and the problems associated with attacking account systems in an organization or individual user account. The multiple facets of password attacks in the system today but we have subjected our study to three main attacks i.e., thus phishing attacks, Man-in-middle attacks, and Brute force attacks. With these specific types of attacks, we will design an approach by using an algorithm to predict and detect possible attacks.

2.1 PASSWORD ATTACKS ON ACCOUNTS

It is believed that the first obvious approach to penetrate the password mechanism is the attempt to find the general method of inverting the encryption algorithm, and this is believed that very possible this can be done but however few successful results have come to light, because the results have not proved to be very useful in penetrating through the system [11]. The Password system simply must be able not only to prevent any access to the system by unauthorized users but must prevent them from logging in at all and must prevent users who are already logged in form doing from doing things they are not authorized to do [12]. Many as discovered, however, another approach is how an attacker tries to keep a potential password until he succeeds, and this insight has been given a general approach name called the Cryptanalytic approach which is otherwise called the Key Search. The attacker has it in his mind that as a human being, being the user of the account, He or She might have the tendency to use a short and simple password at He or she could remember so easily and because of this reason some users use their names, nick nicknames Bers, etc. and this makes the attackers work easier and faster. It has become very common in our world today that people find ways and means to enter people's accounts and that act of social engineering attack as it's been termed is the art of manipulating the people who have less knowledge about these types of attacks such as Phishing and many other types. Most The most organization has security issues that have been of great concern to users, site developers, and specialists, to defend confidential data from this type of social engineering [13]. As several papers have juxtaposed, Passwords can be leaked in multiple way attacker can backpack into the database of the site which stores the user credentials and uncovers a huge number of passwords, this is what is referred auto s Password Theft. Theft can also occur on a personal level. A user can write down the password somewhere and it can make its way to malicious hands, or a user can set a very simple and obvious password that is easy to guess. Social engineering, phishing, or key loggers can also compromise passwords. Passwords can very commonly be uncovered by brute forcing or offline dictionary attacks [14]. A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations 'systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information. Brute force attacks are a common method used by cybercriminals. They accounted for 5% of all data breaches in 2017, according to Verizon research.

2.2 PASSWORD ATTACKS ON ACCOUNT'S INFORMATION SYSTEM

In the field of computer science and its associated data operationalization today, every account user would not be as much happier if he is seen that his or her account in several ways an intrusion for what purpose it is ted to be used for.
Engineers have paid critical attention to this problem and have devised the parameters for determining the strength of a password by account users but with that, it has gotten, its disadvantage both the account and the account holder.
The objective of having a password meter is to provide visual feedback to the user on their choice of a password by labeling it weak, medium, or strong, for example. The criteria for calculating the strength of a password are set by a developer or an institution, such as checking for minimum length, use of dictionary words, and use of special characters. One drawback of this approach is that there is a multitude of varying implementations of password meters, each having its unique set of password rules, which can yield a different result for the same password phrase. The differing results can cause confusion and even distrust by the user. When conflicting feedback for the same password occurs, it decreases a user's trust and willingness to comply with the system [15]. Another drawback is that it is hard to remember such passwords since password meters do not necessarily increase their memorability.
In addition, threats to password accounts or information security plague many industries, and I would one way or the other elaborate more on the effects of this case in the health industry. According to the paper reviewed in this section; The threats against healthcare information systems are growing. Data breaches, generally described as an impermissible use or disclosure of protected health information, are particularly prevalent. Nearly 90% of healthcare organization healthcare served by the Ponemon Institute (which does independent research on privacy, data protection, and information security policy) suffered a data breach in the past 2 years; meanwhile, 64% of organizations reported a successful attack targeting medical files in 2016 a 9% increase in just 1 year. Multiple causative factors are involved in the uptick in attacks against health care healthcare systems, but some reasons cited in that study include low organizational vigilance, inadequate staffing and funding for information technology security, insufficient technology investment, and the underlying value of healthcare data as compared with data from other industries. Attackers use a variety of techniques against

healthcare organizations. Denial of service attacks, aimed at disrupting and disabling systems by overwhelming them with large volumes of network traffic, have targeted healthcare facilities. Such attacks can render clinical systems unusable, with negative effects on core hospital operations, such as delays in surgical procedures, lab-result reporting, and bed management. More recently, attacks against health care healthcare organizations have taken the form of ransomware. In these attacks, an information system, for example, a database containing patient information is encrypted in such a way that only the attacker has the "key" to unlock the data [16].

Similarly, to what I have discussed in the above preliminary points (Navor, 2021) discussed that, although the industry standard of an 8-character password containing 1 upper case, 1 lower case, 1 number, and 1 special character makes for a strong password, an attacker can crack it within a reasonable time. This is dangerous if the password is protecting sensitive information or if the account is integrated into a system with sensitive information. This does not include other security measures that should be considered when designing password security. Proper security implementations can include techniques such as salting to help strengthen passwords and prevent dictionary attacks even if the user develops a weak password. As a user, it is important to keep in mind while you cannot develop the software itself, you can still create a strong password to help yourself or your company defend from attackers should they gain access to the database of passwords. As a system developer or security manager, it is important to train users and inform them of the threats against weak passwords and how to defend against them. Setting up a strong policy that requires a minimum password length and complexity also ensures that passwords cannot be easily brute forced [17]

From the above-discussed points, it is not quite easy when one's organization or individual password account information system is tempered, the challenges of losing a password of your choice are highly bound and possible to happen, and the delays in an organizational functional duty due to lack of accessibility of data information and many more.

2.3 PASSWORD BASED DETECTION MECHANISMS

Password-based attacks are a common attack vector that is used in bypassing or exploiting the authentication of users' accounts. Being one of the most occurring security threats, in 2020 password attacks accounted for 81 data breaches. Password attack entails the exploitation of an authorization vulnerability that is broken in the system alongside a combination of automatic password attack tools that increases the chances of guessing and cracking passwords. The attacker has got several methods of accessing and exposing the credentials that belong to the legal user covering up as the legitimate user by assuming their privileges and identity [18].

Many users on several occasions use the combination of username-password which is one of the oldest methods of account authentication. Therefore, the attackers have got enough time in guessing several methods of getting guessable passwords [19]. Certain applications use passwords as their authentication factor, these applications to are vulnerable to password attacks because the vulnerabilities are properly understood. Password attacks have got serious implications because the users who have malicious intentions only need unauthorized access to one account that they can take advantage of or some accounts for a few users to compromise the web application.

Depending on the nature of the data that is held within an application, passwords that have been compromised can create room for the exposure of information that is sensitive, enhancement of financial fraud, denial of service, and other complicated attacks [20]. Hackers usually depend on various methods of obtaining and authenticating a website using the password of a legitimate user. There are various methods of password attacks which include.

2.3.1 PHISHING ATTACKS

So far, the most widely used technique of password attack is the phishing attack [21]. This technique is a social engineering method whereby the hacker pretends to be a trusted site by sending his or her target a malicious link [22]. After the assumption that they are authenticating to a legal web server, the victim ends up clicking on the link, giving the attacker his or her account details. Under this attack technique, the masquerader usually uses several methods in trapping the victims into clicking the trapping link which include DNS cache poisoning whereby the attacker places vulnerabilities into the application's DNS of the server [23]. This is to redirect the request of the user toward a malicious site with the same-looking domain name [24].

Several password attacks being existing in the current world, and there is a need for the creation of policies that makes users adhere to the set criteria in preventing malicious intruders from hacking their passwords [25]. For example, a password of a legitimate user should have a minimum of 8 characters long and includes special characters to prevent attacks. Passwords used should not have information that is personally identifying. Users should always change their passwords frequently to avoid attacks from using the credential database that has been exposed to password attacks [26].

It is significant for each user to understand the critical nature of a strong password policy and adhere to a huge awareness of password security [27]. Every application user should be aware of social engineering attacks that put them vulnerable to giving out their credentials o unknown people.

The idea of threat detection has many different facets when viewed in the context of a company's security program. Even the greatest security programs need to prepare for adverse circumstances when danger has emerged despite their defense and prevention measures [28].

The first mechanism is having occasional hunts for possible threats. Threat hunts allow security analysts to actively search a company's network implementations, terminals, and security equipment for vulnerabilities or intruders that may be hiding yet unnoticed, as opposed to

waiting for a risk to manifest in the organization's network [29]. This is a sophisticated method that is typically used by seasoned threats and security investigators. All the strategies, in addition to others, should ideally be part of well-designed security threat detection programs to monitor the security of the company's personnel, data, and crucial resources [30].

Next is making use of threat intelligence. This is the method of identifying threats by examining company-specific data from observed assaults and correlating it to the arising corporate data [31]. Because of this, it excels at identifying recognized dangers but not unfamiliar ones. Intrusion Detection Systems, Security Information, and Event Management, web proxy technologies, and antivirus usually make excellent use of threat intelligence [32].

Then, installing intruder triggers is also a strategic mechanism. There are some targets that an attacker simply cannot resist. Because of this, security personnel build traps aiming for the attackers to fall for the set baits. An intruder trap in the environment of a company's network implementation may comprise a specific target that appears to hold network infrastructure that an attacker may find enticing [33]. This includes credentials that appear to hold user rights, which an attacker would require to access private systems or information. The security department receives a notification when an attacker takes advantage of this bait, alerting them that strange behavior on the network needs to be investigated. There are many forms of impersonation technologies that can be implemented in this mechanism [34].

In addition, a company may utilize user behavior analytics to provide a comprehensive overview of what typical employee activity would be in terms of data requirements, geographical locations, and work schedules [35]. In this manner, a spontaneous abnormality in activity, such as login into the system at unexpected hours, shows odd behavior and may require further investigation by a security analyst. The method eliminates the need for a benchmark of activities to compare gathered insights to and instead relies on the possibility that minor, apparently unrelated behaviors for some time on the available company networks may in reality be footprints of activity left by attackers [36]. These parts require cooperation to combine, however, they could assist come up with almost precise ideas of what intruders would be targeted within the corporate network or technological infrastructure.

Lastly, we have the combinatory approach, which demands both a technical aspect and a human factor. Security analysts who examine patterns, trends in data, activities, and analyses are part of the human aspect. They may also decide whether abnormal data points to real threats or just false alarms [37].

3. METHODOLOGY

This Project was implemented by using a Jupiter notebook which is open-source software in which we can create data visualization and other components of the project we used python programming language and machine learning, we used support vector machine algorithm which comes under supervised learning. We choose the KDD datasets which are known for modern internet traffic and have abundant features of distinguishing good and bad connections from the Canadian Institute for Cybersecurity. This dataset has more than 10000 records of good connections and bad connections by using the SVM algorithm, we gave training to the datasets to predict the connections, and we used machine learning libraries to create a data visualization which are graphs and heat maps to explain the prediction of the detection system.

3.1 SVM ALGORITHM

SVM algorithm is a machine learning algorithm that comes under supervised learning which means we train with labeled data which has training data and test data it takes the feedback to improve the result. There are two types of algorithms in supervised-based learning algorithms they are regression and classification.

SVM comes under a classification-based machine learning algorithm that classifies the data based on the features of the dataset.

SVM algorithm makes different from other algorithms due to the boundary line which acts as a no of features if the dataset contains two features the boundary line will be at one line if we continue to add more features to the dataset the boundary line increases its dimension. The data points are more accurate when the distance between the boundary line and values is higher.

STEP 1:

$$c(x, y, f(x)) = \begin{cases} 0, & \text{if } y * f(x) \geq 1 \\ 1 - y * f(x), & \text{else} \end{cases}$$

The cost is 0 if the predicted value and the actual value are of the same sign. If they are not, we then calculate the loss value. We also add a regularization parameter to the cost function. The objective of the regularization parameter is to balance the margin maximization and loss. After adding the regularization parameter, the cost functions look as above.

STEP 2:

$$min_w \lambda \parallel w \parallel^2 + \sum_{i=1}^{n} (1 - y_i \langle x_i, w \rangle)$$

Now that we have the loss function, we take partial derivatives with respect to the weights to find the gradients. Using the gradients, we can update our weights.

STEP 3:

$$\frac{\delta}{\delta w_k}\lambda \parallel w \parallel^2 = 2\lambda w_k$$

$$\frac{\delta}{\delta w_k}\left(1 - y_i\langle x_i, w\rangle\right)_+ = \begin{cases} 0, & \text{if } y_i\langle x_i, w\rangle \geq 1 \\ -y_i x_{ik}, & \text{else} \end{cases}$$

When there is no misclassification, i.e our model correctly predicts the class of our data point, we only have to update the gradient from the regularization parameter.

STEP 4:

$$w = w + \alpha \cdot (y_i \cdot x_i - 2\lambda w)$$

Gradient update -No Classification.
When there is a misclassification, i.e our model makes a mistake on the prediction of the class of our data point, we include the loss along with the regularization parameter to perform a gradient update.

3.2 ALGORITHM

STEP 1:
Input the dataset which consists of network parameters, positive phishing links and negative fishing links and logs to detect the attack.

STEP 2:
Set the priority of the dataset in order to get the accurate score we should implement data cleansing and redundancy to get accurate f1 score.

STEP 3:
SVM algorithm calculates the dataset and gives the result in heatmap and graphs and gives information about the accuracy score.

STEP 4:
In this final step we will implement dataset with other algorithms i.e. kNN and Naive Bayes and compare the score with SVM algorithm

3.3 PURPOSE OF USING THE SVM ALGORITHM

The main purpose of using the SVM algorithm for predicting the connections, the SVM algorithm comes under supervised learning in which we already have the right classification data to train the system to learn the pattern and make the predictions the main application of the SVM algorithm is to predict the data. In this research, we handle the dataset by using data preprocessing and data cleansing to eliminate the redundancies which make the result inaccurate. Also, we have backups of different types of datasets if any dataset does not give accurate results in the predictions and we have a backup of the program if any of the programs do not execute.

Before executing KDD-dataset we tried different types of datasets from Kaggle which is a website having different types of datasets regarding connections and we used different types of algorithms in the execution like the random tree, k-nearest neighbor, and k-mean clustering, and Support Vector Machine algorithms among these algorithms the Support Vector Machine algorithm gives more accuracy compared to other algorithms and Support Vector Classifier is extremely helpful for small datasets.

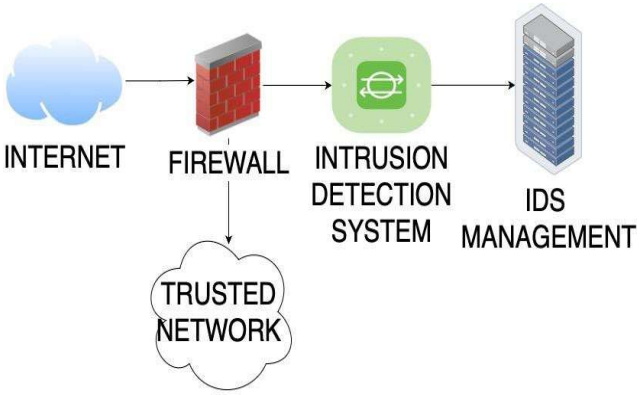

FIG:1 DETECTION SYSTEM

In this detection system, we are using the KDD dataset for predictions because the KDD dataset is known for detecting intrusion activities, we are using SVM algorithms for making predictions.

3.4 SVM CLASSIFIER

A simple SVM classifier works by making a line between two classes and the data points on one side of the line will be classified as a category and the other side will act as another category. This means there can be several lines to choose from. What makes the SVM algorithm better than others because of its choosing line that separates data and is further away from the closest data points as possible. Two closet data points give you support vectors that line is called decision boundary.

After completing the classification, the result is loaded into the decision tree which makes separates it into different categories and makes different sections. After completing the classification in the decision tree, the values are loaded into the prediction section where the results are stored.

4. RESULT AND DISCUSSION

By doing this experiment we created data visualization regarding the number of attacks and the number of protocols. We achieved training accuracy and testing accuracy and greater linear SVM accuracy of “0.916”, created a matrix for predictions on the testing using SVM, prepared a classification report, and established the f1-score which combines the precision and recall of a classifier into a single metric by taking their harmonic mean and we compared to other algorithms like kNN and Naïve Bayes of their f1 score and precision.

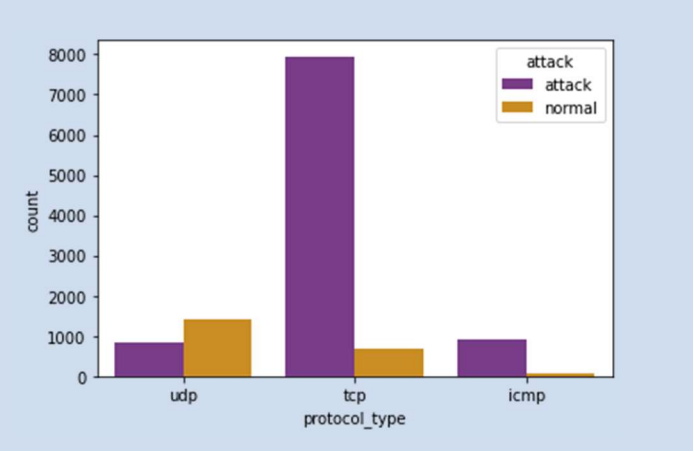

FIG1: Bar graph of protocol type and the number of attacks.

Above graph represents the TCP protocol has the highest number of attacks than UDP and ICMP. TCP doesn't support any data encryption function anyone can gain valuable information. TCP cannot protect against unauthorized access attack.

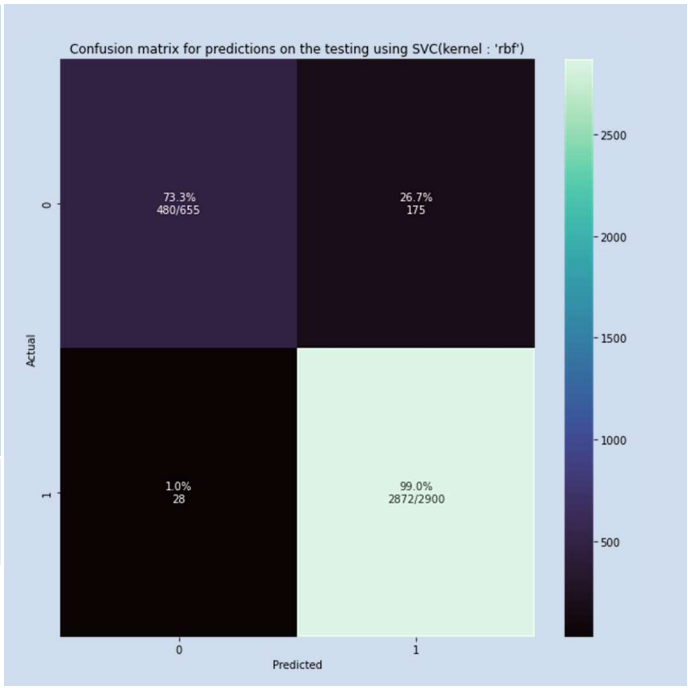

FIG3: Confusion matrix for predictions on testing using SVM Algorithm

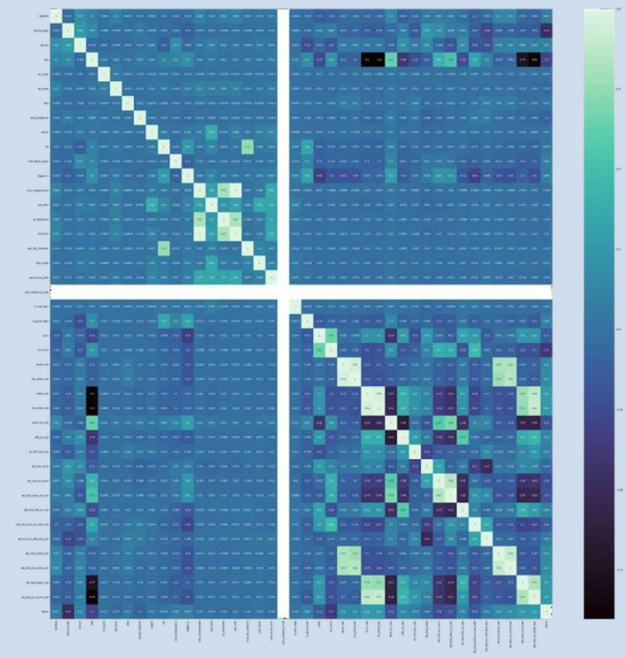

FIG2: Heat map of predictions of attacks on different numbers of parameters

A confusion matrix is a table layout that represents the visualization of the performance of an algorithm. The table divides into four parts True positive, False positive, False Negative, and True Negative. The actual table represents the true positive and false positive, True Negative and False negative.

The above graph shows the different parameters and their probability for detection attacks total of 41 parameters affect the detection attacks.

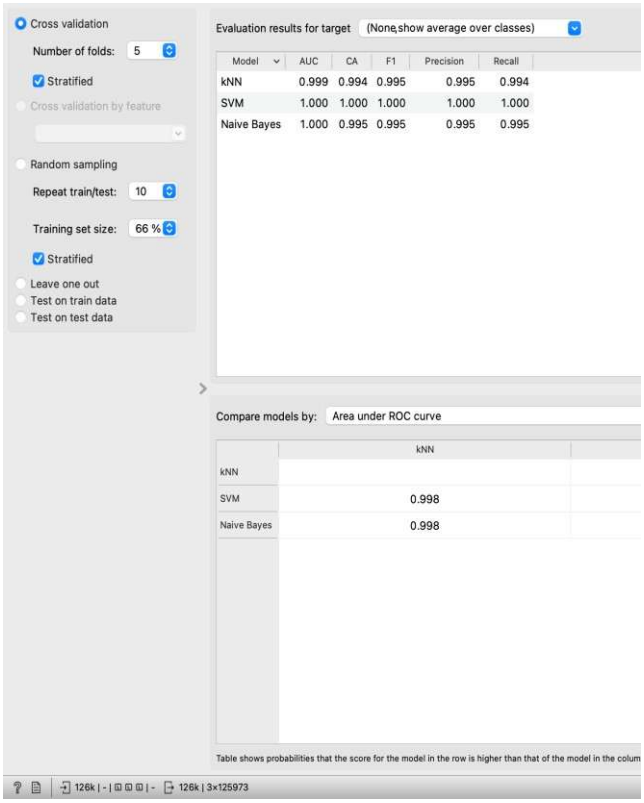

FIG 4: Precision and Recall score for KNN, SVM and Naïve Bayes algorithms.

Above image describes the accuracy and f1 scores about different algorithms which tells which algorithms is more effective for detection

REFERENCES

1. Tasevski, Predrag. "Password attacks and generation strategies." *Tartu University: Faculty of Mathematics and Computer Sciences* (2011).
2. Raza, Mudassar, et al. "A survey of password attacks and comparative analysis on methods for secure authentication." *World applied sciences journal* 19.4 (2012): 439-444.
3. Franchi, Enrico, Agostino Poggi, and Michele Tomaiuolo. "Information and password attacks on social networks: An argument for cryptography." *Journal of Information Technology Research (JITR)* 8.1 (2015): 25-42.
4. Subang, S., and V. Senthooran. "Secure authentication mechanism for resistance to password attacks." *2019 19th International Conference on Advances in ICT for Emerging Regions (ICT)*. Vol. 250. IEEE, 2019.
5. Jansen, Wayne, et al. "Picture password: a visual login technique for mobile devices." *UMBC Student Collection* (2003).
6. Tajpour, Atefeh, Suhaimi Ibrahim, and Maslin Masrom. "SQL injection detection and prevention techniques." *International Journal of Advancements in Computing Technology* 3.7 (2011): 82-91
7. Kadiyala, Sai Praveen, et al. "Securing Microservices Against Password Guess Attacks using Hardware Performance Counters." *2022 IEEE 35th International System-on-Chip Conference (SOCC)*. IEEE, 2022.
8. Tupsamudre, Harshal, et al. "Fixing the Fixes: Assessing the Solutions of SAST Tools for Securing Password Storage." *International Conference on Financial Cryptography and Data Security*. Springer, Cham, 2020.
9. Mostakim, Niaz, Ratna R. Sarkar, and Md Anowar Hossain. "Smart locker: IoT-based intelligent locker with password protection and face detection approach." *International Journal of Wireless and Microwave Technologies* 9.3 (2019): 1-10.
10. WAGHMODE, BABASAHEB. "Web Authentication Password Detection of Network Security Attack Using S-pass." *International Journal of Innovations in Engineering Research and Technology* 4.2: 1-7.
11. Subang S., V. Senthooran, "Secure authentication mechanism for resistance to password attacks. "2019 19th International Conference on Advances in ICT for Emerging Regions (ICT). Vol.250.IEEE,2019.
12. Morris, Robert, and Ken Thompson. "Password security: A case history." Communications of the ACM 22.11(1979): 594-597.
13. Gupta, Surbhi, Abhishek Singhal, and Akanksha Kapoor. "A literature survey on social engineering attacks: Phishing attack." 2016 international conference on computing, communication, and automation (ICCCA). IEEE,2016.
14. Chanda, Katha. "Password security: an analysis of password strengths and vulnerabilities." International Journal of Computer Networks and Information Security 8.7(2016):23.
15. Dupuis, Marc, and Faisal Khan. "Effect of peer feedback on password strength." 2028 APWG symposium on Electric Crime Research (e(Crime). IEEE,2018.
16. Gordon, William j., Adam Fairhall, and Adam Landman. "Threats to information security---public health implications." N Engl J Med 377.8(2017): 707-709.
17. Mayorayor, Preston. "The effects of Password Length and Complexity on Password Resiliency." (2021).
18. Bodkhe, U., Chaklasiya, J., Shah, P., Tanwar, S., & Vora, M. (2020). Markov model for password attack prevention. In *Proceedings of the first international conference on computing, communications, and cyber-security (IC4S 2019)* (pp. 831-843). Springer, Singapore.

19. Subang, S., & Senthooran, V. (2019, September). The secure authentication mechanism for resistance to password attacks. In 2019 19th International Conference on Advances in ICT for Emerging Regions (ICT) (Vol. 250, pp. 1-7). IEEE.

20. Chen, C. M., Wang, K. H., Yeh, K. H., Xiang, B., & Wu, T. Y. (2019). Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications. *Journal of Ambient Intelligence and Humanized Computing*, *10*(8), 3133-3142.

21. Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y., & Ruan, N. (2019). Revealing your mobile password via Wi-Fi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*, *19*(2), 432-449.

22. Pal, B., Daniel, T., Chatterjee, R., & Ristenpart, T. (2019, May). Beyond credential stuffing: Password similarity models using neural networks. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 417-434). IEEE.

23. Aonzo, S., Merlo, A., Tavella, G., & Fratantonio, Y. (2018, October). Phishing attacks on modern android. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1788-1801).

24. Mackie, I., & Yıldırım, M. (2018, July). A novel hybrid password authentication scheme based on text and image. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 182-197). Springer, Cham.

25. Franchi, E., Poggi, A., & Tomaiuolo, M. (2015). Information and password attacks on social networks: An argument for cryptography. *Journal of Information Technology Research (JITR)*, *8*(1), 25-42.

26. Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World applied sciences journal*, *19*(4), 439-444.

27. Niemietz, M., & Schwenk, J. (2012). Ui redressing attacks on android devices. *Black Hat Abu Dhabi*.

28. M. G. Gelles, "Insider threat prevention, detection, and mitigation," *International Handbook of Threat Assessment*, pp. 669–679, 2021.

29. R. Mei, H.-B. Yan, Z.-H. Han, and J.-C. Jiang, "CTSCOPY: Hunting Cyber threats within the enterprise via provenance graph-based analysis," *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*, 2021.

30. A. Oktadika, C. Lim, and K. Erlangga, "Hunting cyber threats in the enterprise using Network Defense Log," *2021 9th International Conference on Information and Communication Technology (ICoICT)*, 2021.

31. P. Koloveas, T. Chantzios, C. Tryfonopoulos, and S. Skiadopoulos, "3. cyber-threat intelligence," *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*, 2022.

32. Ampel, Benjamin, Sagar Samtani, Hongyi Zhu, Steven Ullman, and Hsinchun Chen. "Labeling hacker exploits for proactive cyber threat intelligence: a deep transfer learning approach." In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 1-6. IEEE, 2020.

33. H. M. Lugo-Cordero and R. K. Guha, "What defines an intruder? an intelligent approach," *2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2013.

34. T. Sochor, "Threat detection using honeypots and Honeynets," *Internet Threat Detection Using Honeypots*, pp. 3065–3851.

35. B. Sharma, P. Pokharel, and B. Joshi, "User behavior analytics for anomaly detection using LSTM Autoencoder - insider threat detection," *Proceedings of the 11th International Conference on Advances in Information Technology*, 2020.

36. M. Singh, B. M. Mehtre, and S. Sangeetha, "User behavior profiling using ensemble approach for insider threat detection," *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, 2019.

37. M. G. Gelles, "Insider threat prevention, detection, and mitigation," *International Handbook of Threat Assessment*, pp. 669–679, 2021.

38. Bhattacharya, Tathagata, et al. "Capping carbon emission from green data centers." *International Journal of Energy and Environmental Engineering* (2022): 1-15.

39. Peng, Xiaopu, et al. "Exploiting Renewable Energy and UPS Systems to Reduce Power Consumption in Data Centers." *Big Data Research* 27 (2022): 100306.

40. Bhattacharya, Tathagata, and Xiao Qin. "Modeling Energy Efficiency of Future Green Data centers." *2020 11th International Green and Sustainable Computing Workshops (IGSC)*. IEEE, 2020.

41. Bhattacharya, Tathagata, et al. "Performance modeling for I/O-intensive applications on virtual machines." *Concurrency and Computation: Practice and Experience* 34.10 (2022): e6823.

42. Cao, Ting, et al. "DDoS Detection Systems for Cloud Data Storage." *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2021.

43. Mao, Jianzhou, et al. "Security-Aware Energy Management in Clouds." *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2020.

