MODELING PREDICTING CYBER HACKING BREACHES

Mrs. A SRUTHI PATRO[1], MAJJI JYOTHI[2], MOHAMMED SOHAIL WARIS[3], PUTCHA SRINIVAS MANISH[4], DAMODARA SRIVALLI[5]

[1] Asst. Professor, Department Of Computer Science And Engineering,
RAGHU INSTITUTE OF TECHNOLOGY(AUTONOMOUS)
Affiliated to JNTU GURAJADA, VIZIANAGARAM
Email: sruthi.annepu@raghuenggcollege.in

[2] B.Tech, Department Of Computer Science And Engineering - Cyber Security,
RAGHU INSTITUTE OF TECHNOLOGY(AUTONOMOUS)
Affiliated to JNTU GURAJADA, VIZIANAGARAM
Email: Jyonalli448@gmail.com

[3] B.Tech, Department Of Computer Science And Engineering - Cyber Security,
RAGHU INSTITUTE OF TECHNOLOGY(AUTONOMOUS)
Affiliated to JNTU GURAJADA, VIZIANAGARAM
Email: sohailwaris1712@gmail.com

[4] B.Tech, Department Of Computer Science And Engineering - Cyber Security,
RAGHU INSTITUTE OF TECHNOLOGY(AUTONOMOUS)
Affiliated to JNTU GURAJADA, VIZIANAGARAM
Email: manishbtech53@gmail.com

[5] B.Tech, Department Of Computer Science And Engineering - Cyber Security,
RAGHU INSTITUTE OF TECHNOLOGY(AUTONOMOUS)
Affiliated to JNTU GURAJADA, VIZIANAGARAM
Email: srivalli0813@gmail.com

ABSTRACT

A key technique for improving our comprehension of the development of the threat scenario is the analysis of data sets related to cyber incidents. Numerous investigations need to be conducted because this is a relatively new study issue. In this work, we present a statistical study of a data collection of breach incidents covering 12 years (2005–2017) of malware-related cyberattacks. We demonstrate that, in contrary to the results published in the literature, because hacker breach incidents display autocorrelations, stochastic processes rather than distributions should be used to represent both breach sizes and event inter-arrival periods. Next, specific models of stochastic processes are suggested to suit the breach sizes and the inter-arrival periods, respectively. Furthermore, we demonstrate that the breach sizes and the inter-arrival periods can be predicted by these models. We do both qualitative and quantitative trend studies on the data set to provide deeper insights into the evolution of cyber breach occurrences. We deduce a number of cybersecurity insights, such as the fact that while the frequency of cyberattacks is increasing, the extent of their harm is not.

Keywords: Machine Learning, Support Vector Machine, Django, Masquerader, Cyber Breaches, Scrape data, Interpretation, Authentication, Sequential Query Language, Wamp Server, Regression, Neural Networks, Adding a dataset , classifying using SVM algorithm , Admin access, Analyzing the type of Breaches, Malware Analysis, Un-malware Analysis, Graphical representation of Dataset.

1. INTRODUCTION

Breach scenarios might arise from inappropriate data collection, information loss, or sufficient data leakage. One reason for a data leak might be a program error or lax, non-standard security. Since we can find patterns from these breach instances that happen at specific intervals, our study focuses mostly on identifying and detecting patterns related to cyber hacking breaches. At both the classification and clustering stages, these patterns are identified by utilizing machine learning methods. Given the emphasis on two-way classification and instantaneous trigger action,

classification will be chosen over clustering. Because they are easy to comprehend, classification techniques like logistic regression, decision tree learning, support vector machines, and neural networks are frequently used to identify masqueraders or users who are not verified.

To concentrate on the algorithm's efficacy, we keep a vast collection of website logs for our machine learning algorithms to analyze. Focusing on the model's efficiency is necessary since the issue also maps on time-space tradeoff. It is evident that decision tree learning performs poorly over time, but excels when dealing with outliers. Additionally, the threshold value has a significant bias in logistic regression. The system will fail as a whole if the threshold is lost of control. Although quite sophisticated, neural networks need a large amount of data at first.

The SVM's picture classifications and overall accuracy outperform Decision Trees, and its data needs during early stages of analysis are typically not met. Therefore, we would rather support vector machines with kernels for efficient access pattern categorization on open-access websites for scraping or information extraction. In addition to being easier to grasp than neural networks, support vector machine (SVM) models allow us to convert our data with potential outputs by identifying optimal boundaries through the use of a kernel technique.

1.1 Purpose

The following three contributions are ours. Firstly, we demonstrate that stochastic processes, rather than distributions, should be used to describe both the hacking breach incident sizes and interarrival durations, which indicate the frequency of incidents. It has been observed that the inter-arrival periods of hacking breach instances may be well explained by a certain point procedure.

It is our aim that this study would stimulate more research that will provide an in-depth understanding of alternative strategies for risk minimization. Insurance businesses, governmental organizations, and regulators can benefit from these insights as they must have a thorough understanding of the characteristics of data breach risks.

To help enterprises successfully anticipate, avoid, and reduce cybersecurity threats, cyber hacking breaches are modelled and predicted. Organizations may fortify their defences against cyber threats and shield their vital assets and data from illegal access and exploitation by utilizing predictive analytics, threat intelligence, and proactive risk management techniques.

1.2 SCOPE

Cybersecurity researchers must prioritize modelling and forecasting cyber hacking incidents. To foresee and stop future breaches, the current scope of work entails using a variety of methods and tools to evaluate prior breach data, spot patterns and trends, and create prediction models. The current state of modelling and cyber hacking breach prediction is summarized as follows:

Data Collection and Analysis Organizations collect vast amounts of data related to past hacking breaches, including attack vectors, compromised systems, and outcomes. Advanced analytics tools are used to analyze this data and identify patterns, such as common vulnerabilities exploited by hackers, typical attack timelines, and targeted industries or sectors Constant observation and modification Cyber dangers are always changing, thus in order for prediction models to continue to be useful, they must be continuously monitored. To continually improve prediction models based on fresh data and new threats, organizations use a combination of automated monitoring systems, security analytics platforms, and human experience.

Mitigation and Risk Assessment: By estimating the possibility and possible consequences of cyberattacks, predictive models help companies manage risk. Organizations may reduce risks and lessen the effect of possible breaches by developing incident response plans, implementing targeted security controls, and prioritizing security investments based on the results of these evaluations.

Using threat intelligence, automation, behavioral analytics, advanced analytics, machine learning, and continuous monitoring, cyber threat modeling and prediction encompasses real-time anticipation, detection, and mitigation of cyber attacks. Through the implementation of a proactive and data-driven cybersecurity strategy, entities may fortify their barriers and proficiently guard against constantly changing cyber hazards.

1.3 Motivation

To fortify cybersecurity defenses, mitigate risk, cut expenses, guarantee regulatory compliance, improve incident response capabilities, safeguard sensitive data, and preserve business continuity in the face of changing cyberthreats, modeling and forecasting cyberhacking breaches is done. Organizations may strengthen their defenses against the constantly evolving threat landscape by embracing a proactive and predictive approach to cybersecurity.

The present study is motivated by several questions that have not been investigated until now, such as: Are data breaches caused by cyber attacks increasing, decreasing, or stabilizing? A principled answer to this question will give us a clear insight into the overall situation of cyber threats. This question was not answered by previous studies.

More research that provides in-depth understanding of alternative risk reduction strategies is what we hope this study will spur. Since insurance firms, governmental organizations, and regulators must have a thorough understanding of the nature of data breach risks, these insights are helpful.

1.4 Fundamental concepts Techniques

Data Collection: Gathering relevant data is crucial for modeling cyber hacking breaches. This may include network traffic logs, system event logs, user authentication logs, firewall logs, etc. The data should cover a sufficient time period and include both normal and anomalous activities.

Malware: Malware attacks involve malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Types of malware include viruses, worms, Trojans, ransomware, spyware, adware, and rootkits.

Phishing: Phishing attacks involve sending deceptive emails, messages, or websites that impersonate legitimate entities to trick recipients into providing sensitive information, such as passwords, credit card numbers, or personal data.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: DoS and DDoS attacks aim to disrupt the availability of online services by overwhelming target systems or networks with a flood of traffic, rendering them inaccessible to legitimate users.

Man-in-the-Middle (MitM) Attacks: MitM attacks involve intercepting and altering communication between two parties without their knowledge or consent. Attackers can eavesdrop on sensitive information or manipulate data exchanged between the parties.

SQL Injection: SQL injection attacks exploit vulnerabilities in web applications' input fields to inject malicious SQL queries into the underlying database, allowing attackers to extract, modify, or delete data stored in the database.

Cross-Site Scripting (XSS): XSS attacks involve injecting malicious scripts into web pages viewed by other users, typically through vulnerable web applications. These scripts can steal session cookies, redirect users to malicious websites, or deface web pages.

Network Security Measures:

- Use firewalls to monitor and control incoming and outgoing network traffic, blocking unauthorized access and malicious content.
- Implement intrusion detection and prevention systems (IDPS) to detect and respond to suspicious activities and potential cyber threats in real-time.
- Employ virtual private networks (VPNs) to encrypt data transmitted over public networks, protecting sensitive information from interception by unauthorized parties.
- Segment networks and apply access controls to limit the exposure of critical assets and minimize the impact of a potential breach.

Endpoint Security Solutions:

Install and regularly update antivirus, anti-malware, and anti-spyware software on all endpoints, including desktops, laptops, servers, and mobile devices, to detect and remove malicious software.

Use endpoint detection and response (EDR) solutions to monitor and analyze endpoint activities for signs of compromise, anomalous behaviour, or potential security incidents.

Patch Management:

Regularly update and patch operating systems, applications, and firmware to address

known vulnerabilities and security weaknesses, reducing the risk of exploitation by cyber attackers.

Establish a formal patch management process to prioritize and deploy patches promptly, ensuring timely protection against emerging threats and vulnerabilities.

Secure Configuration and Access Controls:

Implement strong password policies, enforce multi-factor authentication (MFA), and use role-based access controls (RBAC) to limit privileges and restrict access to sensitive systems and data.

Configure devices, applications, and services securely by disabling unnecessary features, ports, and protocols, and enabling encryption, logging, and auditing mechanisms to enhance security posture.

Data Encryption and Backup:

Encrypt sensitive data at rest and in transit using strong encryption algorithms and cryptographic protocols to protect against unauthorized access and data breaches.

Regularly back up critical data to secure and offsite locations, ensuring data availability and integrity in the event of a ransomware attack, data corruption, or system failure.

Security Awareness Training:

Educate employees, contractors, and users about common cyber threats, social engineering tactics, and best practices for cybersecurity hygiene through regular training sessions, awareness campaigns, and simulated phishing exercises.

Foster a culture of cybersecurity awareness and accountability, encouraging employees to report suspicious activities, adhere to security policies, and follow incident response procedures.

2. LITERATURE SURVEY

1 DJANGO – A Python Framework on Web development. Django is a high-level python web framework that encourages rapid development and clean, pragmatic design. This framework consists of many elements which helps the user not to worry about the basic parts and focus on writing the application without any hassle. There are many alternatives for the Django framework in python but what makes it more unique in Django is that it is more secure and it speeds up the development process. Security: Django includes prevention of common attacks like CSRF (cross -site request forgery) and SQL injections. It is very useful for building large web applications. Many software companies use Django as their go-to application. One of such companies is Instagram. Note: Security is essential for any application. Django provides the inbuilt security that includes prevention of common attacks like CSRF (cross-site request forgery) and SQL injections. We've learnt the security topics in Computer Networks[10]. 2.2 Scrapy – Data Extractor from Website Scrapy is a framework which is used to download/get the data from miscellaneous websites. This is usually used for data gathering and data processing. There are several frameworks similar to scrapy. But scrapy is more reliable and robust. Scrapy is a sole framework which has the tools for managing every stage of the web crawl such as request manager, selector, pipelines. 2.3 Beautiful Soup - An Alternate Data Extraction Package Beautiful Soup is a python framework that is used to extract contents from public websites. This python package leverages on the html ids or class of objects. With the reference object, the data referred by the corresponding html package is extracted. The extracted data can be stored in a csv file or json or any other storage documents for analysis. This extraction can also be controlled through security algorithms for the prevention of unwanted hacking breaches. 2.4 Security Algorithms The protection of information in a public website from unwanted scrapping or illegal extraction is a crucial deal in the current digital and social environment. Information plays a major role and matters a lot of money for many business people and website owners. Hence securing the identity, integrity, consistency and maintaining the privacy of the information in websites is of huge interest in today's research. Various encryptions, firewall blocking and other algorithms exist in the literature to act against unauthenticated access. Honeypots are security protocols used to redirect a masquerader to the wrong path. The major focus of our research is to focus on detecting and identifying the patterns pertaining to cyber hacking breaches. These

patterns are recognized by leveraging the machine learning algorithms at both classification and clustering stand points. We prefer classification in place of clustering, as we focus on a two-way classification and immediate triggeraction. Classification techniques including logistic regression, decision tree learning, support vector machines, and neural networks are widely used in detection of the masquerader or unauthenticated users. In order to focus on the effectiveness of the algorithm, we maintain a huge set of logs from the websites for analysis with the machine learning algorithms. Since the problem also maps on time-space tradeoff, there is a need to concentrate on the efficiency of the model [1][5]. It is obvious that decision tree learning works well with outliers but not efficiently with the time. Logistic regression is also heavily biased by the threshold value. Losing control on the threshold will make the entire mechanism to fail. Neural networks are well advanced, but require a good number of data initially. Data requirements during earlier stages of analysis are usually not satisfied. Hence, we prefer support vector machines with kernel for effective classification of access patterns in public websites for information extraction or scrapping.

3. EXISTING SYSTEM

The present study is motivated by several questions that have not been investigated until now, such as: Are data breaches caused by cyber-attacks increasing, decreasing, or stabilizing? A principled answer to this question will give us a clear insight into the overall situation of cyber threats. This question was not answered by previous studies. Specifically, the dataset analyzed in [7] only covered the period from 2000 to 2008 and does not necessarily contain the breach incidents that are caused by cyber-attacks; the dataset analyzed in [9] is more recent but contains two kinds of incidents: negligent breaches (i.e., incidents caused by lost, discarded, stolen devices and other reasons) and malicious breaching. Since negligent breaches represent more human errors than cyber-attacks, we do not consider them in the present study. Because the malicious breaches studied in [9] contain four sub-categories: hacking (including malware), insider, payment card fraud, and unknown, this study will focus on the hacking sub-category (called hacking breach dataset thereafter), while noting that the other three sub-categories are interesting on their own and should be analyzed separately. Recently, researchers started modeling data breach incidents. Maillart and Sornette studied the statistical properties of personal identity losses in the United States between the years 2000 and 2008. They found that the number of breach incidents dramatically increased from 2000 to July 2006 but remained stable thereafter. Edwards et al. analyzed a dataset containing 2,253 breach incidents that span over a decade (2005 to 2015). They found that neither the size nor the frequency of data breaches has increased over the years. Wheatley analyzed a dataset that combined from corresponds to organizational breach incidents between the years 2000 and 2015. They found that the frequency of large breach incidents (the ones that breach more than 50,000 records) occurring to US firms is independent of time, but the frequency of large breach incidents occurring to non-US firms exhibits an increasing trend.

4. PROPOSED SYSTEM

We provide three new contributions in this study. Firstly, we demonstrate that stochastic processes, rather than distributions, should be used to describe both the hacking breach incident sizes and interarrival durations, which indicate the frequency of incidents. The evolution of the hacking breach incidents inter-arrival times can be adequately described by a specific point process, and the evolution of the hacking breach sizes can be adequately described by a specific ARMA-GARCH model (ARMA stands for "Auto-Regressive and Moving Average," and GARCH for "Generalized Auto-Regressive Conditional Heteroskedasticity"). We demonstrate the predictive power of these stochastic process models for both the breach sizes and the inter-arrival times. This is the first article that, as far as we know, demonstrates that these cyber threat elements should be modeled using stochastic processes rather than distributions. Second, we find a positive relationship between the breach sizes and the inter-arrival times of the occurrences, and demonstrate that this dependence can be well characterized by a specific copula. We also demonstrate that the reliance must be taken into account when forecasting inter-arrival

durations and breach sizes, since doing so will lead to inaccurate predictions. This is the first study that, as far as we are aware, demonstrates both the presence of this dependency and the consequences of disregarding it. Third, we do trend studies, both quantitative and qualitative, on the incidences of cyber hacker breaches. The number of hacking breach incidents is increasing, so we find that the situation is getting worse in terms of the incident's inter-arrival time. However, the size of the incident breach is stabilizing, suggesting that the damage from individual hacking breach incidents won't get much worse. Insights into alternative risk reduction strategies can be gained via further research, which is what we hope this study will spur. Because they must have a thorough understanding of the nature of data breach risk, insurance firms, governmental organizations, and regulators can benefit from these insights.

4.1 Proposed Algorithm

SUPPORT VECTOR MACHINE

"Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is the number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot). Support Vectors are simply the coordinates of individual observation. Support Vector Machine is a frontier which best segregates the two classes (hyper-plane/ line). More formally, a support vector machine constructs a hyper plane or set of hyperplanes in a high- or infinite-dimensional space, which can be used for classification, regression, or other tasks like outlier detection. Intuitively, a good separation is achieved by the hyperplane that has the largest distance to the nearest training-data point of any class (so-called functional margin), since in general the larger the margin the lower the generalization error of the classifier. Whereas the original problem may be stated in a finite dimensional space, it often happens that the sets to discriminate are not linearly separable in that space. For this reason, it was proposed that the original finite-dimensional space be mapped into a much higher-dimensional space, presumably making the separation easier in that space.

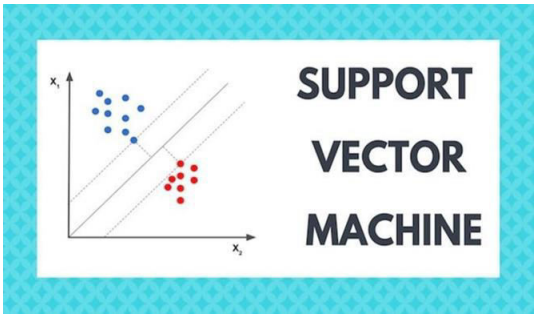

Fig. 4.1.1 Support Vector Machine

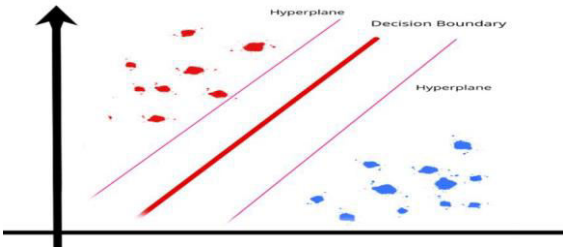

Fig. 4.1.2 SVM Working

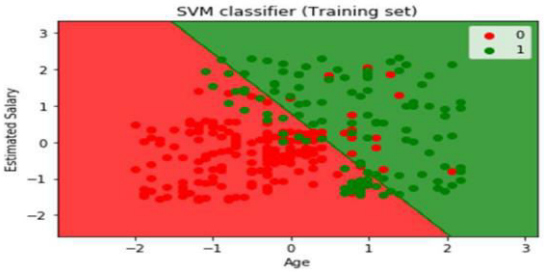

Fig. 4.1.3SVM Testing Classifier

4.2 INPUT AND OUTPUT DESIGN

4.2.1INPUT DESIGN

The interface between the user and the information system is the input design. It includes creating guidelines and protocols for data preparation, which are essential to transforming transaction data into a format that can be processed. This can be done by having users enter data directly into the system or by having the computer read data from a written or printed document. Controlling the quantity of input needed, reducing mistakes, preventing delays, eliminating unnecessary stages, and simplifying the process are the main goals of input design. The input is made in a method that maintains privacy

while offering security and usability. Input Design took into account the following:

- What data should be given as input?
- How should the data be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when errors occur.

OBJECTIVES

1. A user-oriented description of the input is transformed into a computer-based system through the process of input design. The purpose of this design is to prevent mistakes in the data input process and to provide management with the proper guidance for obtaining accurate information from the computerized system.

2. In order to manage massive amounts of data entering, it is accomplished by designing user-friendly interfaces. Making data entering simpler and error-free is the aim of input design. The layout of the data entry panel makes it possible to enter all of the data. It has record viewing capabilities as well.

3. The validity of the data will be checked when it is input. Screens are useful for entering data. In order to prevent the user from becoming stuck in a state of confusion, pertinent messages are sent when necessary. Making an input layout that is simple to understand is, thus, the goal of input design.

4.2.2 OUTPUT DESIGN

An output that satisfies end user criteria and displays information in an understandable manner is considered high quality. Through outputs, processing findings are shared with users and other systems in any given system. In output design, the location of the information for both the hard copy output and the immediate requirement is specified. It is the user's primary and most direct source of information. The system's ability to support user decision-making is enhanced by clever and efficient output design.

1. When designing computer output, one should follow a methodical and well-planned process to ensure that the desired output is produced and that every output component is made in a way that makes the system easy and efficient for users to use. The precise output required to satisfy the criteria should be identified by analyzing design computer output.

2. Select methods for presenting information.

3. Create documents, reports, or other formats that contain information produced by the system.

4. The output form of an information system should accomplish one or more of the following objectives.

i. Convey information about past activities, current status or projections of the

ii. Future.

iii. Signal important events, opportunities, problems, or warnings.

iv. Trigger an action.

v. Confirm an action.

4.3 ARCHITECTURE DIAGRAM

The vulnerabilities in security improvements are widened by technology. In order to get around them, firms that handle a lot of sensitive data have websites and systems that are monitored by firewalls and monitors. Numerous enthusiasts and hackers attempt to compromise the organization's security systems for personal gain or other nefarious purposes. When confidential information is stolen from a website or an organization without authorization, it's called a data breach. When secure or personal data is inadvertently or intentionally obtained from an organization, it is called an information breach. We can train our model to adapt to new conditions and anticipate the next breach by examining the prior efforts, whether they were successful or failed attacks. To protect a website from security breaches, we have developed a machine learning model. In order to display the safe data to take from the internet, we have developed a web application using Django that pulls data from several sources, including Amazon, Flipkart, Snapdeal, and Shopclues. After that, we safeguarded and kept them on our page, making it unlawful for others to remove data from it. Our model will also keep an eye on our website round-the-clock. Every day, the model is taught to produce predictions. The current datasets and the website's history of hacks and breaches will be used to train this model. Current Best Practices: Modern methods of attacking networks remotely using cloud systems include port scanning, DDoS

assaults, botnets, and MITM (man in the middle). Additional types of assaults include those that are focused on storage, applications, and virtual machines[12][13]. The yield sort of a data framework ought to achieve at least one of the following destinations.

- Portray the historical, current and future state of the system
- Raising alerts on events, significant attacks, unwanted activities and vulnerabilities
- Induce and execute appropriate actions on alerts

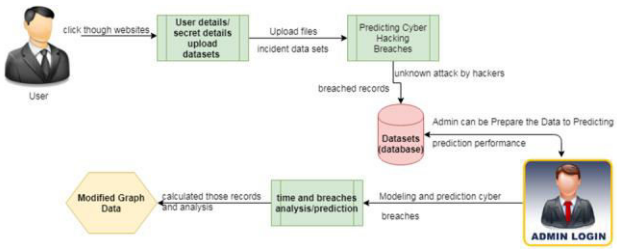

Figure 4.3.1

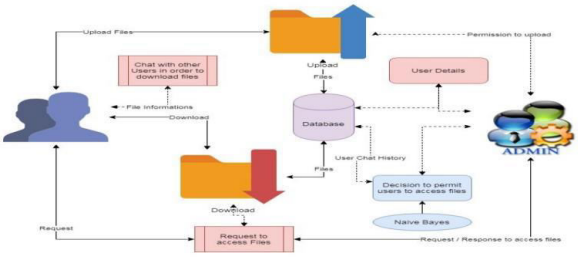

Figure 4.3.2

5. RESULTS

Figure 5.1: The above figure shows the Home Page of the proposed model

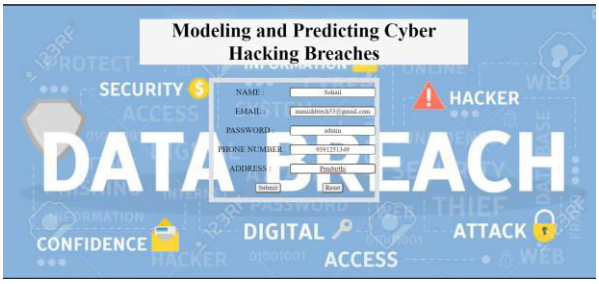

Figure 5.2: The above figure shows the User Login Page of the proposed model

Figure 5.3: The above figure shows the Analysis Page of the proposed model

Figure 5.4: The above figure shows the Un-malware Analysis of the proposed model

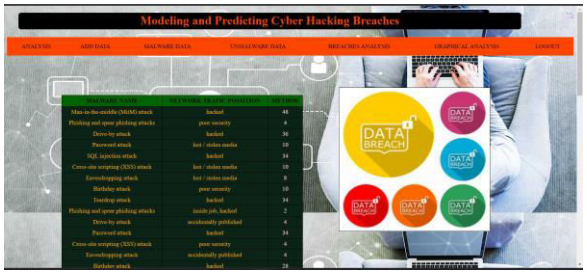

Figure 5.5: The above figure shows the Breaches Analysis of the proposed model

Figure 5.6: The above figure shows the Breaches Analysis column chart of the proposed model

Figure 5.7: The above figure shows the Bar Chart of the proposed model

Figure 5.8: The above figure shows the Spline Chart of the proposed model

6. CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

We examined a dataset of cyber breaches from the perspectives of the extent of the breach and the inter-arrival time of the events, and we demonstrated that both should be characterized by stochastic processes rather than distributions. The statistical models created in this work have acceptable prediction and fitting accuracy. Specifically, we suggest employing a copula-based method to forecast the joint likelihood that an event with a certain breach size would transpire at a later time. According to statistical testing, the approaches suggested in this work outperform those found in the literature since the latter neglected to take into account the temporal correlations and the connection between the incident's breach sizes and inter-arrival periods. To get further insights, we performed both qualitative and quantitative analysis. We came up with a number of cybersecurity observations, one of them being that while the frequency of cyberhacking breach instances is increasing, the sheer extent of their harm is not. Similar datasets can be analyzed using the methods described in this study, or it can be modified.

6.2 FUTURE SCOPE

Numerous unresolved issues remain for further investigation in the future. Examining methods for predicting abnormally high values and handling missing data, such as unreported breach instances, may be both intriguing and difficult. Determining the precise timeframes at which breach occurrences occur is also valuable. In order to comprehend the predictability of breach incidents—that is, the top bound of prediction accuracy—further study is necessary.

7. REFERENCES

[1] Mohammed, Z., 2018. NITDA Raises Alarm over Potential Cyber Attacks to Banks. Govt Agencies, Others Retrieved from. https://www.nigerianews.net/nitdaraisesalarmpotentialcyber-attacks-banks-govt-agencies/.

[2] Nhan, J., Bachmann, M., 2010. Developments in cyber criminology. In: Maguire, M., Okada, D. (Eds.), Critical Issues in Crime and Justice: Thought, Policy, and Practice. Sage, London, pp. 164–183.

[3] Oates, B., 2001. Cyber crime: how technology makes it easy and what to do about it. J. Inf. Syst. Secur. 9(6), 1– 6.

[4] Odunfa, A., 2014. Nigeria: Report on Cyber Threat Calls for Quick Passage of 2012 Bill. Retrieved from. http://www.allafrica.com/stories/201405080279.Html.

[5] Ojedokun, U.A., Eraye, M.C., 2012. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol.

[6] Ojeka, S.A., Ben-Caleb, E., Ekpe, E.-O.I., 2017. Cyber security in the Nigerian banking sector: an appraisal of audit committee effectiveness. Int. Rev. Manag. Market.

[7] (2), 340–346. 7. Okafor, C., 2017. Oracle: Nigerian Banks, Others Lose N127bn Annually to Cybercrime. Oracle. Retrieved from. https://www.thisdaylive.com/index.php/2017/05/14/oracl e-nigerianbanks-others-lose-n127bn-annually-tocybercrime/.

[8] Okamgba, J., 2017. Online Fraud Drains Nigeria over N500 Billion in 7 Years. Retrieved from. https://cfatech.ng/online-fraud-drains-nigeria-over-n500- billion-in-7-years/.
[9] Okoh, J., Chukwueke, E.D., 2016. The Nigerian Cybercrime Act 2015 and its Implication for Financial Institutions and Service Providers. Financier Worldwide.
Retrieved from. https://www.financierworldwide.com/the-nigeriancybercrime-act-2015-and- its-implications-for-financialinstitutions-and-service-providers#.
[10] Olasanmi, O.O., 2010. Computer crimes and counter measures in the Nigerian banking sector. J. Internet Bank. Commer. 15 (1), 1–10.
[11] Olawoyin, O., 2017. North Korean Hackers Attack Banks in Nigeria, 17 Other Countries – Kaspersky. Premium Times Retrieved from.
https://www.premiumtimesng.com/news/topnews/22816 6-north-korean-hackers-attack-banks-in-nigeria-17-othercountries-kspersky.html.
[12] Olayemi, O.J., 2014. A socio-technological analysis of cybercrime and cyber security in Nigeria. Int. J. Sociol. Anthropol. 6 (3), 116–125.
[13] Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., Esan, A.O., 2016. Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE J. Eng. Technol. 1 (1), 37–42.
[14] Omotubora, A.O., 2016. Comparative perspectives on cybercrime legislation in Nigeria and the UK-a case for revisiting the" hacking" offences under the Nigerian Cybercrime Act 2015. Eur. J. Law Technol. 7 (3), 1–15.
[15] Oni, A.A., Ayo, C.K., 2010. An empirical investigation of the level of users' acceptance of ebanking in Nigeria. J. Internet Bank. Commer. 15, 1–13.
[16] T Manikandan, B Balamurugan, C Senthilkumar, RRA Harinarayan, RR Subramanian, “Cyber War is Coming”, Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, John Wiley & Sons, Inc, pp. 79-89, Mar. 2019 .