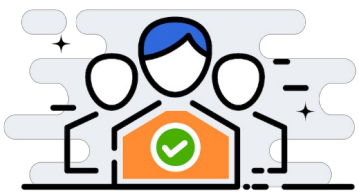
WISEN
IT SOLUTIONS
Progressive Quality Thinking

Table of Contents



Abbreviation

DNS	Domain Name Server
DoH	DNS over HTTPS
HTTP	Hyper Text Transfer Protocol
NTP	Network Time Protocol
UDP	User Datagram Protocol

Base Paper Title

Defense Strategies for Epidemic Cyber Security Threats Modeling and Analysis by Using a Machine Learning Approach

Modified Title

Improving Robustness and Effective DNS Attack Detection using Neural Network

Modified Title Explanation

Improving Robustness:: Close the gap in model performance

Effective:: Can detect multiple type of DDoS Attack on DNS Server

Neural Network:: A Deep Learning Model

Abstract

Distributed Denial-of-Service (DDoS) attacks exhaust resources, leaving a server unavailable to legitimate clients. The Domain Name System (DNS) is a frequent target of DDoS attacks. Since DNS is a critical infrastructure service, protecting it from DoS is imperative. Many prior approaches have focused on specific filters or anti-spoofing techniques to protect generic services. DNS root nameservers are more challenging to protect, since they use fixed IP addresses, serve very diverse clients and requests, receive predominantly UDP traffic that can be

spoofed, and must guarantee high quality of service.

This attack is made by leveraging the Domain Name System (DNS) technology through Domain Generation Algorithms (DGAs), a stealthy connection strategy that yet leaves suspicious data patterns. To detect such threats, advances in their analysis have been made. For the majority, they found Deep Learning (DL) as a solution, which can be highly effective in analyzing and classifying massive amounts of data. Although strongly performing, ML models have a certain degree of obscurity in their decision-making process. To cope with this problem, a branch of DL known as Explainable DL tries to break down the black-box nature of classifiers and make them interpretable and human-readable.

Our analysis reveals that the approach was successful in inferring significant DNS amplification DDoS activities including the recent prominent attack that targeted one of the largest anti-spam organizations. Moreover, the analysis disclosed the mechanism of such DNS amplification DDoS attacks.

Introduction

The Domain Name System (DNS) service is one of the core services in the internet functionality. Distributed Denial of Service (DDoS) attacks on DNS service typically consist of many queries coming from a large botnet. These queries are sent to the root name server or an authoritative name server along the domain chain. The targeted name server receives a high volume of requests, which may degrade its performance or disable it completely. Such attacks may also contain spoofed source addresses resulting in a reflection of the attack or may send requests that generate large responses (such as an ANY request) to use the DNS for amplification attacks. According to Akamais state of the internet report nearly 20% of DDoS attacks in Q1 of 2016 involved the DNS service. Moreover, even some of the Internets DNS root name servers were targeted.

One type of particularly hard to mitigate DDoS attacks are randomized attacks on the DNS service. In these attacks, queries for many different non-existent subdomains (subkeys) of the same primary domain (key) are issued). Since the result of a query to a new subdomain is not cached at the DNS resolver, these queries are propagated to the domain authoritative server, overloading both these servers and the open resolvers of the Internet Service Provider

Domain name system (DNS) is one of the most important technologies of the Internet. We can convert a domain name into an IP address using DNS. Without this service, the Internet would not be deployed as widely as it is now. DNS messages are normally built on top of UDP packets. Unlike in TCP, it is easy to forge the source address of UDP packets. As a result, DNS requests with a fake source address can easily be sent to a DNS server. In theory, any DNS server can answer any domain name resolution request; there are no protocol requirements that limit or filter request messages from client nodes. When DNS was invented, malicious activity utilizing DNS servers as packet reflectors was not extensive; however, as the Internet grew, attackers started to use this open operating policy to send traffic to victim nodes by forging DNS message source addresses. To prevent this activity, recent DNS servers have been configured to answer requests originating only from specific client nodes, typically filtered by source IP address. Unfortunately, there are more than a few improperly configured DNS

servers in the wild; these are called open resolvers. The DNS protocol is still one of the major methods for attacking.

The Domain Name System (DNS) is a global, hierarchical, distributed database which serves, among other things, to map domain names to Internet Protocol (IP) addresses. While relatively straight forward in concept, in practice the global DNS is complex to the point of being arcane . For the purpose of this paper, we introduce a limited scope and vocabulary; the interested reader can find more depth in the operation and security of DNS in and . The domain name system operates as a query-response protocol, in which a query for a fully qualified domain name (FQDN) is made by a client, or endpoint, and is answered via an iterative process known as resolution. An FQDN is made up of a series of text labels separated by periods. For example, the FQDN www.google.com has three labels [www, google, com].

From a hierarchical perspective, the right-most label in an FQDN is the top-level-domain (TLD) and the each subsequent label represents a subdomain of the FQDN created from all the prior labels. For instance www.google.com is a subdomain of google.com, which in turn is a subdomain of com. The term domain is often used to refer to both an FQDN and the scope of its possible subdomains. Thus www.google.com, mail.google.com, inbox.google.com, and photo.google.com are all subdomains of the domain google.com. The TLD is a single label and is considered public in the sense that its subdomains are available for registration and not controlled by the TLD. The TLDs are limited in number and controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). In some cases, subdomains of a TLD are also managed as public domains, most notably domains like co.uk, and are considered public suffixes and create extended TLDs (eTLD).2 A second-level-domain (SLD) is privately owned and the direct subdomain of a public suffix, or eTLD. Examples of second-level-domains include google.com and google.co.uk. The SLD is sometimes referred to as the base domain.

Within the Domain Name System, authoritative name servers are servers which hold authoritative, or definitive, answers for a certain portion of the database, generally a specific domain. If these authoritative servers are not functioning properly, Internet traffic to the domains for which they are authoritative may be interrupted or completely disrupted. For this reason, companies often have multiple authoritative name servers for their domains.

While it is possible for an endpoint to resolve DNS queries themselves, in practice, most devices rely on large recursive resolvers to perform resolution on their behalf. Internet Service Providers provide recursive resolvers for their customers, for example. Many recursive resolvers are configured to answer queries only for devices in their network, thereby limiting the resource demands on those network appliances. There are public resolvers, such as those operated by Google, openDNS, and Cloudflare, designed to handle recursion for any endpoint selecting their service.3 On the other hand, there are also a large number of devices on the Internet that, through misconfiguration or otherwise, will act as recursive resolvers for any client but are not announced as public resolvers. These are known as open resolvers and are frequently leveraged by cyber actors to anonymize and amplify DDoS traffic.

Enterprises typically host various kinds of DNS assets. They will typically host a small number of recursive resolvers that proxy DNS requests from internal hosts to external DNS servers, and also cache results to reduce the number of external queries. Individual hosts may choose to over-ride the enterprise recursive resolvers, such as by manually changing their preferred resolver to a public one (such as Googles 8.8.8.8 and CloudFlares 1.1.1.1),

but in general, a majority of hosts will use the default recursive resolver provided by their organization. In addition, enterprises typically host a number of authoritative name servers to serve the various domains belonging to the organization. For example, organization-wide services (like email, VPN, etc.) may be managed by central IT. At the same time, each department may operate its own authoritative name server to resolve department-specific web pages. It is not uncommon for the various IT entities to operate in silos, often unaware of the assets being managed by the other. To make matters worse, on-campus retail stores (bookshops, food outlets, etc.) that lease connectivity from the campus may also be housing their own DNS assets, which are often poorly secured as they lack the skills.

Distributed-Denial-of-Service (DDoS) attacks remain a serious problem, in spite of decades of research and commercial efforts to curb them. Ongoing Covid19 pandemic and increased reliance of our society on network services, have further increased opportunities for DDoS attacks. According to the security company F5 Labs, between January 2020 and March 2021, DDoS attacks have increased by 55% . While some large-volume DDoS attacks make front page news (for example, the 1.35 Tb/s attack on Github in Feb. 2018, or 2021 17.2 M requests per second attack, detected by CloudFlare), many more attacks occur daily and disrupt operations of thousands of targets.

Denial of Service (DoS) attacks pose a major, omnipresent threat to the stability of the Internet. About one-third of the active /24 networks on the Internet received DoS attacks over a two-year period , and 90% of attacks mitigated at a large IXP involved reflection attacks. To bring about reflection, attackers spoof source IP addresses to send request packets that supposedly originate from an intended victim, and abuse the infrastructure that replies to these requests (e.g., open DNS resolvers). Amplification is successful if the responses are larger than the requests. The DNS is a core Internet component. It primarily operates over the transport-layer protocol UDP. Due to its stateless nature, UDP is particularly susceptible to spoofing, and at least 14 protocols that work on top of UDP allow for reflection attacks. The Network Time Protocol (NTP) and DNS are (currently) the most-abused protocols.

Notably, amplification attacks are not limited to UDP. Poor implementations of network stacks allow attackers to use TCP as well. A recent DNS amplification attack exploits inefficient resolver implementations and works regardless of the underlying transport-layer protocol DNS amplification remains one of the most popular attack vectors, despite recent changes such as DNS-over-TLS and DNS-over-HTTPS.

A classic form of DDoS attacks still common in todays networks is the TCP SYN Attack. In this form of attack, the attacker initiates many TCP connections, while never completing the TCP handshake. The connection queue of the target is therefore filled up with incomplete connections, preventing it from addressing new connection requests from legitimate parties. The attacker may make an attack more difficult to detect by utilizing a botnet or a large army of sources for carrying out the attack or even by simply using spoofed sources. In this case, the attacked destination receives connection requests from many different sources.

Expert measurement methods are essential to observe global attack activities. Having a thorough understanding of attack dynamics and the abused infrastructure is crucial to effectively mitigate DNS-based attacks and to reduce the opportunity for infrastructure abuse. Several efforts exist to monitor amplification attacks on a global scale. Primarily, the monitoring infrastructures are implemented with the help of honeypots. In such works, careful assumptions are made about the share of global attacks that honeypots account for because the

amplification ecosystem consists of a large number of amplifiers with high churn rates. Moreover, sophisticated attackers learn about the location of honeypots and exclude them.

There are multiple ways of describing the taxonomy and types of DDoS attacks, having different sources both from academia and business approaching the problem of taxonomy differently. Mirkovic and Reiher divide the different types in classes based on specific criteria that are both technical and social, e.g. based on the impact of the attack. Some of the criteria are degree of automation (DA), exploited weakness to deny service (EW), source address validity (SAV), attack rate dynamics (ARD), possibility of characterization (PC), persistence of agent set (PAS), victim type (VT) and impact on the victim (IV). On the other hand, the NIST provides only two types of DDoS attacks, flaw exploitation and flooding. The main distinction between the two types lies in the medium used to perform the attack and the end-system being attacked. In the flaw exploitation, the target is the software of the system, attempting to deplete its resources like memory, CPU, disk space or memory buffers. In flooding attacks, the attack is on the networking capabilities of the target, depleting the network capacity by accessing the resource with the means of attack, thus making it inaccessible for legitimate users.

Threats of malware, attacks and intrusion have been around since the very conception of computing. Yet, it was not until the sudden growth of the internet that awareness of security and digital assets really started to pick up steam. The internet presents a new liability, as the everincreasing number of machines on the web provides a new goldmine for those seeking to exploit vulnerabilities. As access increases, new ways are created for attackers to exploit network systems and their users. Among various types of attack, DDoS remains the most devastating and severe due to its potential impact, and the potentiality keeps on growing, making intrusion detection a must for network security and defense. As a result, machine learning and artificial intelligence research has flourished over the last few years, opening new doors for intrusion detection technologies. However, data availability still limits greatly the success of such technologies, as research faces a shortage of good quality IDS datasets.

During the last decades, our day-by-day life has been strictly connected to the usage of devices and online services, therefore making their efficiency and continuity play a crucial role in the technological transformation we witness. Likewise, the economic loss derived from cyberthreats has increased exponentially in recent years as the technologies continually evolve and attackers develop their skills. One of the most common ways cybercriminals try to jeopardize the continuity of systems and thus cause economic damage is Denial of Service (DoS), which aims to drain the computing capabilities of the target system in both fancy and basic ways. A case of this attack is the Distributed Denial of Service DDoS, where a network of infected devices (bots) are commanded by an attacker (botmaster) through a Command&Control Server (C&C). What happens to be erratic and thus detectable by a Machine Learning (ML) model in this kind of attack is the DNS traffic, carrying Domain Names through which bots are connected to the C&C server. This stealthy connection strategy is commonly known as Domain Fluxing, where the algorithms used by the infected bots to generate the domain are known as Domain Generation Algorithms (DGAs).

Although employing ML models to detect the presence of botnets within network traffic has been demonstrated to be successful, almost the entirety of the relevant works have followed a common baseline and workflow, presenting a partially novel feature set on which to train a classifier to obtain relevant results. The proposed approaches lack interpretability and contextualization. First, depending on the context from which DNS traffic data is extracted and the model is deployed, potential attackers might have control over some features. Second, the model prioritization and general usage of the features in the decision process are not known beforehand,

making the process challenging to debug and protect.

Motivation

Motivated by a recent new type of randomized Distributed Denial of Service (DDoS) attacks on the Domain Name Service (DNS), we develop novel and efficient distinct deep algorithms and build an attack identification system that uses our algorithms.

Objectives

- How to infer large-scale DNS amplification DDoS activities?
- What are the characteristics of DNS amplification DDoS attacks?
- What inferences can we extract from analyzing DNS amplification DDoS traces?
- Which explain ability techniques can provide insight into how the model takes its decisions?
- How to train different classifiers and compare their performances?

Problem Statement

The relevance of the results achieved from such techniques rely on the quality of the datasets employed, as these are vital to have a realistic evaluation. The validity of current datasets has been thoroughly questioned in the cybersecurity space. It is a challenge for many researchers to find appropriate datasets to validate and test their methods and having a suitable dataset is a significant challenge itself. Privacy is a huge setback for availability of these datasets as they contain sensitive information. In the off chance that these are made available, they are heavily anonymized or obsolete. The unavailability of such datasets and the absence of certain statistical characteristics remains one of the major challenges for anomaly-based intrusion detection.

The nature of the datasets brings about data privacy issues due to certain security policies, the sensitivity of the data and the potential risk from disclosing such information. Moreover, there are other trust factors that inhibit realistic data from being shared among industry stakeholders and researchers. As a result, organisations often choose to not disclose the outcomes of computer attacks. Therefore, most researchers do not use realistic data when conducting their own studies

A thorough review of literature is carried out to analyze three key areas: the use of Deep learning in the context of intrusion detection; the state-of-the art of datasets, their characteristics and shortcomings; and, a review of recent works on the validity of existing datasets. This lays the groundwork for the problem definition and objective of this study, that is, to analyze the intrusion detection performance of DDoS datasets.

Existing System

This paper investigates the mathematical modelling of cybercrime attacks on multiple devices connected to the server. This model is a very successful way for cybercrime, bio-mathematics, and artificial intelligence to investigate and comprehend the behaviour of mannerisms with harmful intentions in a computer system. In this computational model, the existing system authors are studying the factors (i.e., computer viruses, disease infections, and cyberattacks) that affect connected devices. This compartmental model, SEIAR, represents the various hardware utilised during the cyberattack. The letters S, E, I, A, and R are used to represent different stages or groups of individuals in epidemiological models, helping to understand the spread and control of infectious diseases. The dynamics of the previous model are determined by a series of differential equations. The dynamics of the preceding model are determined by a system of differential equations. Numerical solutions of the model are calculated using backpropagated Levenberg-Marquardt algorithm (BLMA) and a specific optimization algorithm known as the Levenberg-Marquardt algorithm (LMA). Reference solutions were obtained by using the Runge-Kutta algorithm of order 4 (RK-4). The backpropagated Levenberg-Marquardt algorithm (BLMA), commonly known as the damped least-squares (DLS) method. Subsequently, the existing system authors endeavor to analyze the surrogate solutions obtained for the system and determine the stability of our approach. Moreover, the existing system authors aim to ascertain fitting curves to the target solutions with minimum errors and achieve a regression value of 1 for all the predicted solutions. The outcome of our simulations ensures that our approach is capable of making precise predictions concerning the behavior of real-world phenomena under varying circumstances. The testing, validation, and training of our technique concerning the reference solutions are then used to determine the accuracy of the surrogate solutions obtained by BLMA. Convergence analysis, error histograms, regression analysis, and curve fitting were used for each differential equation to examine the robustness and accuracy of the design strategy.

In this work, the existing system authors use one of the intelligent techniques based on an artificial neural network to investigate the mathematical model that simulates Pony Stealer (malware attack) in the connection that has been developed. The mathematical model is compartmental since asymptomatic devices, as well as Exposed Susceptible, Susceptible, Infectious, and Recovered, have all been regarded as separate systems linked by a single server. Some infections can propagate through asymptomatic devices without causing symptoms. These viruses are identified through infectious devices. This extra type of device is crucial to include in cyber security models since many cyberattacks are intended to control the device system in an anonymous manner in order to collect personal data [68]. Such real-world processes are regulated by a set of ordinary differential equations. Deep neural learning-based machine learning techniques [69], have been applied to solve the system of ordinary differential equations underlying the epidemic model. In the ANN approach, the existing system authors use one hidden layer for sample points of each equation in Matlab, and using the RK-4 approach, a reference solution is generated, which is later analysed using the Levenberg-Marquardt algorithms training, testing, and validation procedures. Since the approximate solutions and analytical answers correspond with the lowest absolute errors when compared to state-of- the-art techniques, the detailed graphical analysis shows that the suggested method is accurate and effective. Additionally, performance indicator values are getting closer to zero, demonstrating flawless outcome modelling. VII. CONFLICTS OF INTEREST The author declare no conflicts of

interest.

Drawbacks of Existing System

- Narrowly specialized knowledge
- Cannot meet current network business demands
- High complexity, inaccuracy, and inadequacy
- High complexity of installing and maintaining
- Makes fine-grained source-IP filtering much harder.

Dataset Desc

Dataset URL: https://data.mendeley.com/datasets/bzgf9r36kp

Dataset Description:

Distributed Denial of Service (DDoS) is one of the most frequent attacks in cloud that cause significant damage, affect the performance and continue to be the predominant security challenge. Over the past decade, research on DDoS attack detection has focused on a few classes of these attacks.

To generate DDoS flooding attack we use three tools namely: hping3, mausezahn and wreckuests. UDP flood attack, TCP SYN flood attack and ICMP flood attack was performed by using hping3. For DNS flood attack mausezahn was used and for HTTP Flood attack wreckuests was used. Tcpdump, a traffic protocol analyzer is used to capture the attack traffic. Moreover, legitimate traffic was also collected using tcpdump from Lab environment network. The captured attack traffic and normal traffic were used to create a new dataset. The dataset has six classes and 1081633 records out of which 1001984 are DDoS attacks.

Proposed System

Our goal is to design an AI brain, which continuously evaluates suitability of multiple filters to handle an ongoing DDoS attack on a DNS root server. Our system needs to quickly select the best filter or the combination of filters, reasoning about the projected impact on the attack, the collateral damage from the filter on legitimate recursive traffic and the operational cost. The system should also be able to adjust its selection as attack changes. Finally, individual filters need to be configured to achieve optimal performance high effectiveness against attacks they are designed to detect and low collateral damage.

Feature Statistical Analysis. These plots show the marginal distributions of every pair of features as density plots,

describing how the distributions for the classes behave. Through the scattered plots instead, we can assess where both benign and malicious samples lie in their adhoc feature space, thus making us capable of understanding to which extent pairs of features separate the data. Analyzing the scattered plots allows observing the distribution of the features to get a rough idea of how they will behave/discriminate and to which extent.

Features considered to incorporate time series elements of the attacks included averaging descriptive statistics such as minimum or maximum of different components, e.g., labels or prefix lengths, per minute over an attack, as well as variance and co-variance measures. While promising, these features proved more difficult to assess and scale given the volume of data and were not used in the final clustering. Given the strong time elements in DDoS attacks, improved approaches to leveraging time series features at scale would likely prove valuable to understanding the malware and actors.

We propose a method of classifying a DNS server, according to whether or not it is used as a reflector, by monitoring the incoming DNS messages. We collect a series of DNS packets sent from a DNS server and build a feature matrix of the server, assuming that a reflector may have a different packet sequence pattern than that found with a normal DNS server. The preliminary result shows that our method can classify reflectors with an F1 score greater than 0.9 when the test and training data are generated within the same day. The trained model can also classify the data not used for the training and testing phase of the same day with more than 0.7 F1 score.

Advantages of Proposed System

- Its not difficult to see what is Impacted
- Simple, fast and less complex.
- Excellent empirical performance
- Streamlined and decoupled services
- Simple to use and interpret

Hardware & Software Requirements

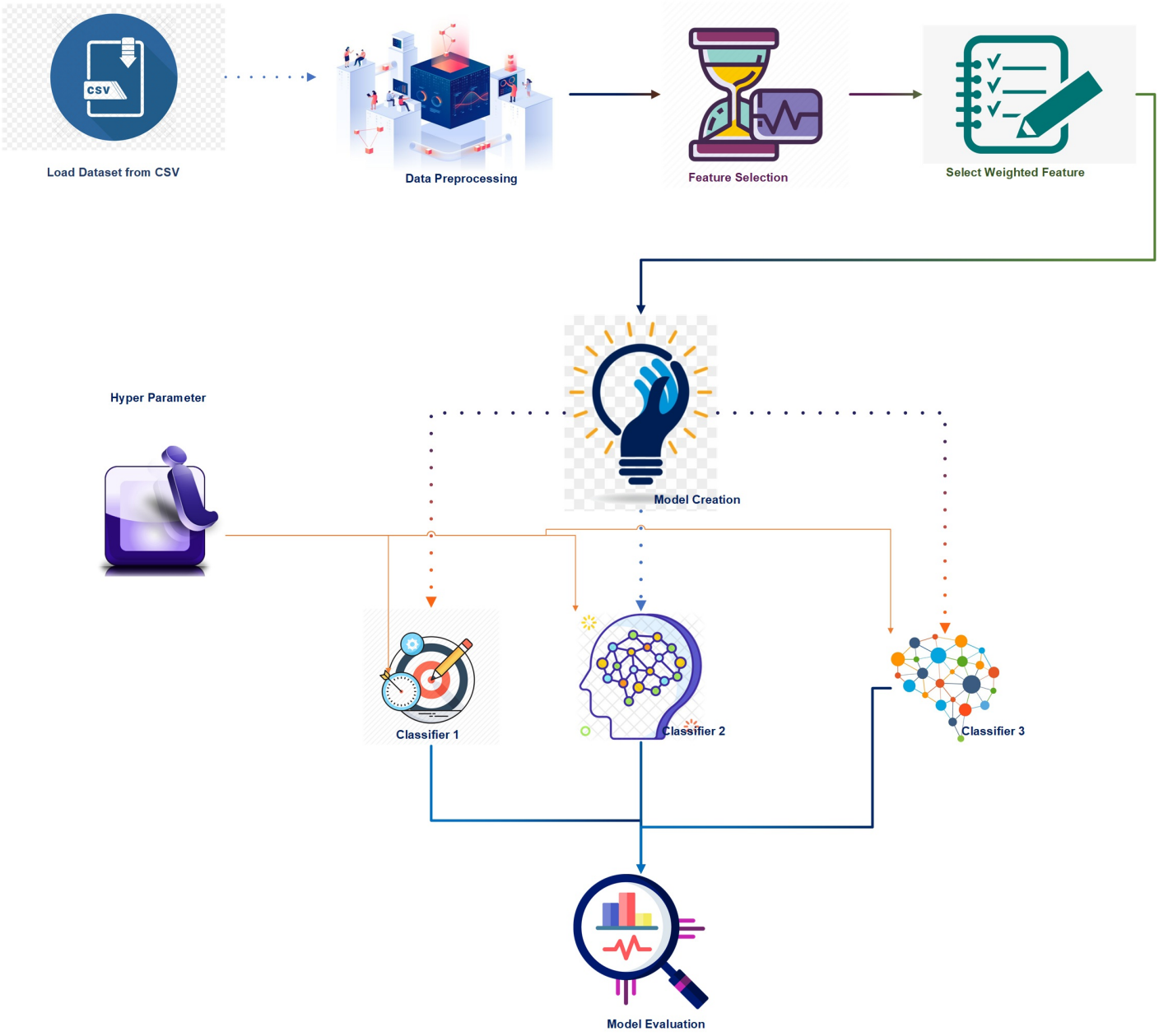
Hardware Requirements

- Processor: Minimum i3 Dual Core
- Ethernet connection (LAN) OR a wireless adapter (Wi-Fi)
- Hard Drive: Minimum 100 GB; Recommended 200 GB or more
- Memory (RAM): Minimum 8 GB; Recommended 32 GB or above

Software Requirements

- Python
- Anaconda
- Jupyter Notebook
- TensorFlow
- Keras

Architecture



Existing Algorithm

- Machine Learning Algorithm

Proposed Algorithm

- Long Short Term Memory (LSTM) Algorithm

Advantages of Proposed Algorithm

Long Short Term Memory (LSTM) Algorithm Advantages Advantages

- Can be used when dealing with large sequences and accuracy is concerned.
- Improved method of back propagating the error.
- Explicitly designed to deal with the long-term dependency problem.

Project Modules

Module 1 : Exploratory Data Analysis

EDA is associated with graphical visualization techniques to identify data patterns and comparative data analysis. EDA is a preferred technique for feature engineering and feature selection processes for data science projects. Some of the widely used EDA techniques are univariate analysis, bivariate analysis, multivariate analysis, bar chart, box plot, pie carat, line graph, frequency table, histogram, and scatter plots. We use EDA to quickly identify any errors in the data. In the Univariate Analysis, we perform data analysis on a single variable. In the Multivariate Analysis, we perform comparative analysis between multiple variables. For any machine learning and deep learning projects, finding data correlations using visual representations is key to identifying dataset insights. Therefore, we explores these insights to set the right path to achieving the accurate model prediction goals.

Module 2 : Feature Selection

In our study of relevant features we employ three standard selection methods: correlation-based univariate, MI-based univariate, and correlationbased forward search algorithms. Correlation (MI) based univariate methods simply rank features based on their correlation (MI) with the target variable. Then the desired number of features is selected based on the ranking. Forward search correlation-based method iteratively selects features based on maximum relevance and minimum redundancy. The relevance is calculated based on the correlation between the feature and the target variable while redundancy is calculated based on the correlation between the feature and the previously selected subset of features.

Module 3 : Model Training and Evaluation

Splitting Datasets: A key characteristic of a good learning model is its ability to generalise to new, or unseen, data. A model which is too close to a particular set of data is described as overfit, and therefore, will not perform well with unseen data. A generalised model requires exposure to multiple variations of input samples. Primarily, models require two sets of data, one to train and another to test. The training data is the set of instances that the model trains on, while the testing data is used to evaluate the generalisability of the model, that is, the performance of the model with unseen data. The train/test split can yield good results; however, this approach has some drawbacks. Although splitting is random, it can happen that the split creates imbalance between the

training and the testing set, where the training set has a large number of instances from only one class. In such cases, the model fails to generalise and overfits.

To mitigate this, the datasets are split into three subsets; training, validation and testing. This split is done in a 60:20:20 ratio, for training, validation and testing respectively. The train_test_split helper method from the scikit-learn library is used for the split. With this approach, training is done in two phases, with the training and the validation sets. Firstly, the training set is used to train the model. Then, the validation set is used to estimate the performance of the model on unseen data (data that the model is not trained on).

Parameter Tuning: A parameter can be loosely described as a pre-defined attribute of the data. A parametric algorithm possesses a fixed number of parameters. While a parametric algorithm is computationally more efficient, it makes stronger assumptions about the dataset. This would be ideal if the assumptions are correct. However, parametric algorithms perform poorly with incorrect assumption.

In contrast, non-parametric algorithms are more flexible. In nonparametric scenarios, as the algorithm learns, the number of parameters grows. This type of algorithm performs slower computations; however, it makes far less assumptions about the dataset.

Literature Survey

Literature Survey 1	
Title	How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond
Authors	Nan Sun , Chang-Tsun Li , Hin Chan , Md Zahidul Islam , Md Rafiqul Islam and Warren Armstrong
Published Year	2022
Efficiency	Excellent empirical performance Improve the quality and consistency of data Minimizes the workload on infrastructures.
Drawbacks	May take huge time and economic cost to construct. Maximizes the complexity of the problem Narrowly specialized knowledge
Description	Cyber assurance, which is the ability to operate under the onslaught of cyber attacks and other unexpected events, is essential for organizations facing inundating security threats on a daily basis. Organizations usually employ multiple strategies to conduct risk management to achieve cyber assurance. Utilizing cybersecurity standards and certifications can provide guidance for vendors to design and manufacture secure Information and Communication Technology (ICT) products as well as provide a level of assurance of the security functionality of the products for consumers. Hence, employing security standards and certifications is an effective strategy for risk management and cyber assurance. In this work, we begin with investigating the adoption of cybersecurity standards and certifications by surveying 258 participants from organizations across various countries and sectors. Specifically, we identify adoption barriers of the Common Criteria through the designed questionnaire. Taking into account the seven identified adoption barriers, we show the recommendations for promoting cybersecurity standards and certifications. Moreover, beyond cybersecurity standards and certifications, we shed light on other risk management strategies devised by our participants, which provides directions on cybersecurity approaches for enhancing cyber assurance in organizations. In this work, we presented the results of our survey on the Common Criteria adoption and approaches to ensuring cyber assurance for organizations. To determine if organizations have concerns related to cybersecurity regulatory issues as well as to determine organizations attitudes towards being measured against cybersecurity standards, seven adoption barriers of security standards and certications are identied. The results of our study inform our recommendations for pro- moting Common Criteria adoption and broader cybersecurity standards and certications. Aside from the use of cybersecu- rity standards and certications to select secure ICT products, we investigate how organizations pursue cyber assurance and their adopted strategies. We hope the ndings and recommen- dations we have made help researchers, organizations, and regulators raise concerns among academia and industry about the importance of cybersecurity standards and certications. Beyond cybersecurity standards and certications, the survey presents insights and directions on risk management, in the hope of

	inspiring organizations to achieve cyber assurance.

Literature Survey 2	
Title	A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations
Authors	Alladean Chidukwani , Sebastian Zander and Polychronis Koutsakis
Published Year	2022
Efficiency	👍 Better operational efficiency 👍 Performs better on various circumstances and environment 👍 Improved reliability and resilience
Drawbacks	👎 Maximizes the complexity of the problem 👎 May take huge time and economic cost to construct. 👎 Resulting data errors.
Description	Small-to-medium sized businesses (SMBs) constitute a large fraction of many countries economies but according to the literature SMBs are not adequately implementing cyber security which leaves them susceptible to cyber-attacks. Furthermore, research in cyber security is rarely focused on SMBs, despite them representing a large proportion of businesses. In this paper we review recent research on the cyber security of SMBs, with a focus on the alignment of this research to the popular NIST Cyber Security Framework (CSF). From the literature we also summarise the key challenges SMBs face in implementing good cyber security and conclude with key recommendations on how to implement good cyber security. We find that research in SMB cyber security is mainly qualitative analysis and narrowly focused on the Identify and Protect functions of the NIST CSF with very little work on the other existing functions. SMBs should have the ability to detect, respond and recover from cyber-attacks, and if research lacks in those areas, then SMBs may have little guidance on how to act. Future research in SMB cyber security should be more balanced and researchers should adopt well-established powerful quantitative research approaches to refine and test research whilst governments and academia are urged to invest in incentivising researchers to expand their research focus. Continuous on-going research is required to support the development of cyber security solutions for SMBs [15], [102]. Research in cyber security is however rarely focussed on SMBs, despite them representing a large proportion of business. SMBs contribute immensely to the global econ- omy, and in particular in Australia they make up 98% of all businesses contributing one third of the GDP. Despite their large number and importance, our study shows that research in SMB cyber security is rather limited and narrowly focussed. This is consistent with previous ndings of other researchers [15]. We also found SMB cyber security research to be con- centrated in the USA despite other nations having similar high proportions of SMBs and facing similar threats but in different environments.

Literature Survey 3	
Title	Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach
Authors	Abdul Wahid Khan , Shah Zaib , Faheem Khan , Ilhan Tarimer , Jung Taek Seo and Jiho Shin
Published Year	2022
Efficiency	👍 Computational Complexity is significantly reduced 👍 Eliminating the huge workload of traditional methods 👍 May not meet the real-time requirement.
Drawbacks	👎 Big payloads 👎 Unsuitable for large scale scenarios. 👎 High complexity of installing and maintaining
Description	Security is the protection from various kinds of threats and most organizations engage in the challenge of security especially cyber-attacks. The attacks are increasing rapidly, due to which cyber security does not now change on supervised and pattern-based detection algorithms which assure continuous security observing. There are many kinds of problems in vendor organizations like cyber theft, which is the most common attack in cyberspace. This research study is developing a Cyber Security Challenges Model (CSCM) that will facilitate vendors organizations to identify challenges of cyber security during the development of software in a vendor organization. To find cyber security issues/challenges, a Systematic Literature Review (SLR) is conducted on 44 relevant research publications by developing a search string based on research questions. As the final selected research publications were less in number and did not complete our aim, therefore, snow bowling technique is applied to 67 relevant research publications. This relevant data was comprised of different databases/sources e.g., Google Scholar, IEEE Explore, SpringerLink, ACM Digital Library, anFffid ScienceDirect. Furthermore, for the distinctive literature review, weve carried out all of the steps in SLR, for example, improvement of SLR protocol, initials, and a very last collection of the applicable information, data extraction, data quality assessment, and data synthesis. Thirteen (13) critical cyber security challenges are identified which are; Security issues/Access of Cyberattacks, Lack of Right Knowledge, Framework, Lack of Technical Support, Disaster Issues, Cost Security issues, Lack of Confidentiality and Trust, Lack of Management, Unauthorized Access issues, Lack of Resources, Lack of Metrics, Administrative Mistakes during Development and Lack of Quality, Liability, and Reliability. The findings of our analysis study signify the similarities and dissimilarities in the recognized cybersecurity challenges in different decades, companies/firms, continents, databases, and methodologies. Through SLR, we have identied a list of 13 challenges which are all marked as critical challenges for vendor orga- nization during software development in CSCM as shown in (48%), D (43%), E (40%), F (39%), G (37%), H (33%), I (31%), J (28%), K (28%), L (27%) and M (25%). The vendor organizations need to give proper attention to these critical challenges to avoid any risk of failure by addressing these challenges.

Literature Survey 4	
Title	Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks
Authors	Abdul Basit Ajmal , Masoom Alam , Awais Abdul Khaliq , Shawal Khan , Zakria Qadir and M. A. Parvez Mahmud
Published Year	2021
Efficiency	👍 Quick and Efficient to use 👍 Delivering information on the state of operation. 👍 Fast and efficient, but also as accurate as the state-of-the-art algorithms
Drawbacks	👎 High complexity of installing and maintaining 👎 They are hard to maintain 👎 Complexity of its Real Time Implementation
Description	There exists a gap between existing security mechanisms and their ability to detect advancing threats. Antivirus and EDR (End Point Detection and Response) aim to detect and prevent threats; such security mechanisms are reactive. This approach did not prove to be effective in protecting against stealthy attacks. SCADA (Supervisory Control and Data Acquisition) security is crucial for any country. However, SCADA is always an easy target for adversaries due to a lack of security for heterogeneous devices. An attack on SCADA is mainly considered a national-level threat. Recent research on SCADA security has not considered unknown threats, which has left a gap in security. The proactive approach, such as threat hunting, is the need of the hour. In this research, we investigated that threat hunting in conjunction with cyber deception and kill chain has countervailing effects on detecting SCADA threats and mitigating them. We have used the concept of decoy farm in the SCADA network, where all attacks are engaged. Moreover, we present a novel threat detection and prevention approach for SCADA, focusing on unknown threats. To test the effectiveness of approach, we emulated several SCADA, Linux and Windows based attacks on a simulated SCADA network. We have concluded that our approach detects and prevents the attacker before using the current reactive approach and security mechanism for SCADA with enhanced protection for heterogeneous devices. The results and experiments show that the proposed threat hunting approach has significantly improved the threat detection ability. Due to the change of threat landscape, reactive approaches are ineffective in detecting and reacting in time, resulting in no detection or increasing duel time between incident response and attack. Proactive approaches in conjunction with decep- tion and threat intelligence are an effective way of detect- ing and preventing threats quickly and using SCADA decoy farm to engage in attack and record its activity by providing IOCs to threat hunters. Hence we concluded that the threat detection ability of SCADA is increased using the threat hunting approach against real-world attacks as compared to traditional security mechanisms. For future directions, Our future work includes Adversary simulation on networks to mature our threat hunting teams with regular adversary exercises.

Literature Survey 5	
Title	A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units
Authors	Haichun Zhang , Yuqian Pan , Zhaojun Lu , Jie Wang and Zhenglin Liu
Published Year	2021
Efficiency	👍 Simplify the implementation process. 👍 Effectiveness for distributed optimization 👍 Achieve a well-balanced tradeoff among various parameters.
Drawbacks	👎 Generally have high polynomial running times. 👎 Narrowly specialized knowledge 👎 It is not an easy-to-use method
Description	Modern vehicles are equipped with more than 100 Electrical Control Units (ECUs) with over 2500 signals to transmit internally. The application of advanced electronics and communication techniques helps a vehicle transform from an information island into a powerful distribution center. However, a large number of ECUs have introduced a wider range of security threats for vehicles. The attackers can compromise a vehicle remotely through a vulnerable ECU. How to evaluate the cyber security of in-vehicle ECUs has become an important issue. Current Threat Analysis and Risk Assessment (TARA) only carries out theoretical analysis on the potential threats and risks faced by the vehicle in the conceptual design phase of the lifecycle, but lacks the details of actual security evaluation. In this paper, we proposed a Cyber Security Evaluation Framework (CSEF) to independently evaluate the security of the in-vehicle ECUs, which is composed of the asset identification, the threat analysis, the risk assessment, and the security test. The proposed CSEF is applied to a pre-installed On-Bord Unit (OBU) to provide a use case. The use case show that the proposed CSEF is able to figure out assets, threats, risks behind threats, and vulnerabilities of OBU, playing an important role in guiding others to conduct security evaluation. Moreover, CSEF can be extended to evaluate the cyber security of other critical ECUs, such as the Telematic Box, the infotainment units, and the gateway. In order to better apply the security assessment to the IoV, we analyzed the security architecture of the IoV in detail, and proposed a security framework for the IoV. The security framework focuses on ten security aspects of smart vehicles and in-vehicle ECUs at four levels, which regulates the scope of security evaluation. In addition, we proposed CSEF that can be applied to in-vehicle ECUs to evaluate the cyber security of in-vehicle ECUs.The CSEF is designed based on the ISO/SAE 21434 standard and is optimized to have richer security assessment details, which can be better applied to the eld of automotive security. The framework aims to solve ve main problems:(1) identies the assets of the evaluated objectives from ten aspects.

Literature Survey 6	
Title	A Review of Security Standards and Frameworks for IoT-Based Smart Environments
Authors	Nickson M. Karie , Nor Masri Sahri , Wencheng Yang , Craig Valli and Victor R. Kebande
Published Year	2021
Efficiency	👍 Effectiveness for distributed optimization 👍 Ability To Deliver High Quality Results 👍 Capable of further reducing the required level of human effort
Drawbacks	👎 They are hard to maintain 👎 Prone to Errors 👎 Generally have high polynomial running times.
Description	Assessing the security of IoT-based smart environments such as smart homes and smart cities is becoming fundamentally essential to implementing the correct control measures and effectively reducing security threats and risks brought about by deploying IoT-based smart technologies. The problem, however, is in finding security standards and assessment frameworks that best meets the security requirements as well as comprehensively assesses and exposes the security posture of IoT-based smart environments. To explore this gap, this paper presents a review of existing security standards and assessment frameworks which also includes several NIST special publications on security techniques highlighting their primary areas of focus to uncover those that can potentially address some of the security needs of IoT-based smart environments. Cumulatively a total of 80 ISO/IEC security standards, 32 ETSI standards and 37 different conventional security assessment frameworks which included 7 NIST special publications on security techniques were reviewed. To present an all-inclusive and up-to-date state-of-the-art research, the review process considered both published security standards and assessment frameworks as well as those under development. The findings show that most of the conventional security standards and assessment frameworks do not directly address the security needs of IoT-based smart environments but have the potential to be adapted into IoT-based smart environments. With this insight into the state-of-the-art research on security standards and assessment frameworks, this study helps advance the IoT field by opening new research directions as well as opportunities for developing new security standards and assessment frameworks that will address future IoT-based smart environments security concerns. This paper also discusses open problems and challenges related to IoT-based smart environments security issues. As a new contribution, a taxonomy of challenges for IoT-based smart environment security concerns drawn from the extensive literature examined during this study is proposed in this paper which also maps the identified challenges to potential proposed solutions.

Literature Survey 7	
Title	Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation
Authors	Abdul Basit Ajmal , Munam Ali Shah , Carsten Maple , Muhammad Nabeel Asghar and Saif Ul Islam
Published Year	2021
Efficiency	👍 Simplify the implementation process. 👍 Better operational efficiency 👍 Keeping the control overhead at regular levels
Drawbacks	👎 Faces critical design challenges. 👎 Heavyweight 👎 Approach is a bit time-consuming
Description	Attackers increasingly seek to compromise organizations and their critical data with advanced stealthy methods, often utilising legitimate tools. In the main, organisations employ reactive approaches for cyber security, focused on rectifying immediate incidents and preventing repeat attacks, through protections such as vulnerability assessment and penetration testing (VAPT) security information and event management (SIEM), firewalls, anti-spam/anti-malware solutions and system patches. Such system have weaknesses in addressing modern modern stealthy attacks. Proactive approaches, have been seen as part of the solution to this problem. However, approaches such as VAPT have limited scope and only works with threats that have already been discovered. Promising methods such as threat hunting are gaining momentum, enabling organisations to identify and rapidly respond to any potential attacks, though they have been criticised for their significant cost. In this paper, we present a novel hybrid model for uncovering tactics, techniques, and procedures (TTPs) through offensive security, specifically threat hunting via adversary emulation. The proposed technique is based on a novel approach of inducing adversary emulation (mapping each respective phase) model inside the threat hunting approach. The experimental results show that the proposed approach uses threat hunting via adversary emulation and has countervailing effects on hunting advance level threats. Moreover, the threat detection ability of the proposed approach utilizes minimum resources. The proposed approach can be used to develop the offensive security-aware environment for organizations to uncover advanced attack mechanisms and test their ability for attack detection. This paper has presented a novel hybrid model for launch- ing offensive security exercises to capture, determine and understand attack patterns by foreseen threats using threat hunting. The proposed approach has increased the efciency of identifying and countering threats using real world attack scenarios and presents an algorithm to generate attack vectors for phishing. In contrast to traditional methods that focus on known threats, such as VAPT. The proposed scheme is designed to identify and address emerging unknown threats. In the future, we plan to focus on increasing the realism of the emulation of adversaries with advanced stealthy attacks.

Literature Survey 8	
Title	Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security
Authors	Abel Yeboah-Ofori , Shareeful Islam , Sin Wee Lee , Zia Ush Shamszaman , Khan Muhammad , Meteb Altaf and Mabrook S. Al-Rakhami
Published Year	2021
Efficiency	Quick and Efficient to use Increased efficiency and speed Low Deployment Cost
Drawbacks	Difficulties to obtain better performance High complexity of installing and maintaining Cannot be implemented real time
Description	Cyber Supply Chain (CSC) system is complex which involves different sub-systems performing various tasks. Security in supply chain is challenging due to the inherent vulnerabilities and threats from any part of the system which can be exploited at any point within the supply chain. This can cause a severe disruption on the overall business continuity. Therefore, it is paramount important to understand and predicate the threats so that organization can undertake necessary control measures for the supply chain security. Cyber Threat Intelligence (CTI) provides an intelligence analysis to discover unknown to known threats using various properties including threat actor skill and motivation, Tactics, Techniques, and Procedure (TT and P), and Indicator of Compromise (IoC). This paper aims to analyse and predicate threats to improve cyber supply chain security. We have applied Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques to analyse and predict the threats based on the CTI properties. That allows to identify the inherent CSC vulnerabilities so that appropriate control actions can be undertaken for the overall cybersecurity improvement. To demonstrate the applicability of our approach, CTI data is gathered and a number of ML algorithms, i.e., Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT), are used to develop predictive analytics using the Microsoft Malware Prediction dataset. The experiment considers attack and TTP as input parameters and vulnerabilities and Indicators of compromise (IoC) as output parameters. The results relating to the prediction reveal that Spyware/Ransomware and spear phishing are the most predictable threats in CSC. We have also recommended relevant controls to tackle these threats. We advocate using CTI data for the ML predicate model for the overall CSC cyber security improvement. The integration of complex cyber physical infrastructures and applications in a CSC environment have brought eco- nomic, business, and societal impact for both national and global context in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. However, CPS security remains a challenge as vulnerability from any part of the system can pose risk within the overall supply chain context. This paper aims to improve CSC security by integrating CTI and ML for the threat analysis and predication.

Literature Survey 9	
Title	Factors Related to Cyber Security Behavior
Authors	Ana Kovaevi , Nenad Putnik and Oliver Tokovi
Published Year	2020
Efficiency	Found attractive outcomes Provides the integrity and nontransferablity. Relatively simple and computationally inexpensive method
Drawbacks	High complexity of installing and maintaining Heavyweight Solutions have been proved ineffective
Description	Theoretical and empirical insight notes that cyber security awareness is a topic of particular interest in cyber security. Humans are the central figures in cyber security and the way to reduce risk in cyberspace is to make people more security aware. While there have been numerous studies about various aspects of cyber security awareness, they are both inconsistent and environment-dependent. The main aim of our research is to analyze cyber security awareness in depth, and to try to discover how various factors such as socio-demographics, cyber security perceptions, previous cyber security breaches, IT usage, and knowledge may individually or together impact on cyber security behavior. To prove that we conducted our research on students, as they are the most technologically active part of the society. We discovered that knowledge proved to be the dominant factor for cyber security awareness, and although students are digital natives, they do not feel safe in the cyber environment; they do not behave securely and do not have adequate knowledge to protect themselves in cyberspace. The environment is a very important factor when analyzing cyber security, as stated in [15], and this is the rst sur- vey conducted among university students in Serbia (in par- ticular freshmen), which analyzes the factors relevant for cyber security awareness in depth. In addition, our survey also analyzed unreported correlations; how various factors in A. Kovaevi et al.: Factors Related to Cyber Security Behavior particular and together, such as socio-demographic character- istics, cyber security perceptions, cyber security breach expe- riences, IT usage, and knowledge inuence security behavior. It was shown that the effects of cyber security perceptions, knowledge, and experiences are stronger than the effects of socio-demographics for cell phone related behavior, or in particular, IT usage and knowledge appeared as signicant predictors of cell phone related behavior. However, any sig- nicant predictors have not been discovered for password related behavior, which will be the focus of our future anal- ysis. Even though our participants perceived that their data were not safe, this did not serve as a trigger for them to learn more about cyber security so as to nd out how to behave more securely in cyberspace.

Literature Survey 10	
Title	A Risk Management Approach to Double-Virus Tradeoff Problem
Authors	Jichao Bi , Fangfei Zhang , Ali Dorri , Chunming Zhang and Chen Zhang
Published Year	2019
Efficiency	Simplify the implementation process. Fast and efficient, but also as accurate as the state-of-the-art algorithms Lowering the Complexity Threshold
Drawbacks	Approach is a bit time-consuming Resulting data errors. Generally have high polynomial running times.
Description	One of the major threats to cybersecurity is the emergence of new computer viruses. By emergence of new viruses, the cybersecurity companies assign a team of security experts and programmers to study the behavior of the virus and develop the corresponding antivirus program to secure networks. Sometimes, more than one new virus is identified that requires the cybersecurity team to make a tradeoff on the allocation of programmers, and thus leads to two-antivirus-program development problem under double-virus attack. In this paper, we propose DOWNHILL algorithm to address the outlined challenge. We model the time evolution of the expected state of the network as a differential dynamical system to measure the total loss caused by the viruses. Then, we propose a DOWNHILL algorithm, three heuristic algorithms and a random algorithm to solve the problem, respectively. We study the computational complexities of the proposed algorithms as well. Through numerous comparative experiments, we confirm the DOWNHILL algorithm is the most effective method to this problem. Finally, the influence of different factors on the DOWNHILL strategy and its potential total loss are also researched. In the framework of risk management, this paper studied the computer virus response problem. On this basis, we modeled the problem of tackling with new viruses as a two-antivirus- program development problem. The latter is dened as how to allocate the limited programmer resources to develop dif- ferent antivirus programs to achieve the minimum potential total loss (caused by viruses). Through modeling and anal- ysis of the time evolution of the networks expected state, we quantied the networks potential loss caused by Virus I and II, respectively. Then, we obtained the potential total loss by adding them together. We presented DOWNHILL algorithm to solve this problem. The simulation results prove that the proposed DOWNHILL algorithm achieves better performance as compared to three heuristic algorithms and the random algorithm. We also studied the impact of multiple factors on DOWNHILL strategy. To the best of our knowl- edge, this work is the rst work that studies the double-virus tradeoff problem.

Conclusion

While the absence of datasets was the very focal point at which this study was conducted, it can also be seen as a limitation on its own given the fact that potentially more accurate results would have been obtained on the comparison between the datasets.

Our attack detection method for public peering points has enabled us to unveil distributed inter-domain attacks. Our results show that the DNS attack vector is more popular than previously captured by (even distributed) honeypots, a common vantage point in the context of reflection and amplification attacks. We were successful in tracking a prominent attack entity and identifying concrete attack patterns. Our study reveals that attackers are able to detect new abusable amplifiers quickly and reasonably change which infrastructure they abuse. At the same time, we find that attackers could achieve higher amplification by choosing (query) names more prudently. especially in the case of attacks utilizing spoofing and highly variable amplifier sets.

There were a number of time-related features that we did not capture in our clustering, but found particularly compelling. Some generators appear to use a fixed number of labels at any time, which changes over the attack, presumably from building attack queries by continually appending, or removing, labels. In this particular example, the number of labels descends in time, but in many other examples it is seen to ascend. This would be consistent with the use of a dictionary, which is used to select a label, and creating queries by continually appending labels.

Future Work

There are numerous avenues for further research into this area the results of which can help us understand cyber actors better and may lead to techniques that can be applied to a broader set of problems. In our research, we did not study the victims, for example, which may further refine our understanding of both the generators and the actors operating these attacks. One could take a number of graph approaches to these problems, including a study of how the labels form tightly connected clusters among attacks.

References

» Muhammad Sulaiman,Muhammad Waseem,Addisu Negash Ali,Ghaylen Laouini,Fahad Sameer Alshammari Defense Strategies for Epidemic Cyber Security Threats: Modeling and Analysis by Using a Machine Learning Approach IEEE Access, 2024

» Jichao Bi,Fangfei Zhang,Ali Dorri,Chunming Zhang,Chen Zhang A Risk Management Approach to Double-Virus Tradeoff Problem IEEE Access, 2019

» Abdul Basit Ajmal,Munam Ali Shah,Carsten Maple,Muhammad Nabeel Asghar,Saif Ul Islam Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation IEEE Access, 2021

» Abel Yeboah-Ofori,Shareeful Islam,Sin Wee Lee,Zia Ush Shamszaman,Khan Muhammad,Meteb Altaf,Mabrook S. Al-Rakhami Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security IEEE Access, 2021

» Ana Kovacevic,Nenad Putnik,Oliver ToÅ¡kovic Factors Related to Cyber Security Behavior IEEE Access, 2020

» Nan Sun,Chang-Tsun Li,Hin Chan,Md Zahidul Islam,Md Rafiqul Islam,Warren Armstrong How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond IEEE Access, 2022

» Haichun Zhang,Yuqian Pan,Zhaojun Lu,Jie Wang,Zhenglin Liu A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units IEEE Access, 2021

» Alladean Chidukwani,Sebastian Zander,Polychronis Koutsakis A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations IEEE Access, 2022

» Abdul Basit Ajmal,Masoom Alam,Awais Abdul Khaliq,Shawal Khan,Zakria Qadir,M. A. Parvez Mahmud Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks IEEE Access, 2021

» Abdul Wahid Khan,Shah Zaib,Faheem Khan,Ilhan Tarimer,Jung Taek Seo,Jiho Shin Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach IEEE Access, 2022

» O. David, S. Sarkar, N. Kammerer, C. Nantermoz, F. M. de Chamisso, B. Meden, et al., Digital assistances in remote operations for ITER test blanket system replacement: An experimental validation, Fusion Eng. Des., vol. 188, Mar. 2023.

» P. Xiao, Z. Qin, D. Chen, N. Zhang, Y. Ding, F. Deng, et al., FastNet: A lightweight convolutional neural network for tumors fast identification in mobile-computer-assisted devices, IEEE Internet Things J., vol. 10, no. 11, pp. 9878-9891, Jun. 2023.

» A. S. Alsafran, A feasibility study of implementing IEEE 1547 and IEEE 2030 standards for microgrid in the kingdom of Saudi Arabia, Energies, vol. 16, no. 4, pp. 1777, Feb. 2023.

» R. Pinciroli and C. Trubiani, Performance analysis of fault-tolerant multi-agent coordination mechanisms, IEEE Trans. Ind. Informat., vol. 19, no. 9, pp. 9821-9832, Sep. 2023.

» M. Aizat, A. Azmin and W. Rahiman, A survey on navigation approaches for automated guided vehicle robots in dynamic surrounding, IEEE Access, vol. 11, pp. 33934-33955, 2023.

» M. Jalili and M. Perc, Information cascades in complex networks, J. Complex Netw., vol. 5, pp. 665-693, 2017.

» P. SzÃµr, The Art of Computer Virus Research and Defense, Hagerstown, MD, USA:Pearson, 2005.

» M. H. R. Khouzani, S. Sarkar and E. Altman, Optimal dissemination of security patches in mobile wireless networks, IEEE Trans. Inf. Theory, vol. 58, no. 7, pp. 4714-4732, Jul. 2012.

» S. Eshghi, M. H. R. Khouzani, S. Sarkar and S. S. Venkatesh, Optimal patching in clustered malware epidemics, IEEE/ACM Trans. Netw., vol. 24, no. 1, pp. 283-298, Feb. 2014.

» C. Nowzari, V. M. Preciado and G. J. Pappas, Analysis and control of epidemics: A survey of spreading processes on complex networks, IEEE Control Syst., vol. 36, no. 1, pp. 26-46, Feb. 2016.

» H. Lin and N. W. Bergmann, IoT privacy and security challenges for smart home environments, Information, vol. 7, no. 3, pp. 44, 2016.

» N. M. Karie, N. M. Sahri and P. Haskell-Dowland, IoT threat detection advances challenges and future directions, Proc. IEEE Workshop Emerg. Technol. Secur. IoT (ETSecIoT), pp. 22-29, Apr. 2020.

» V. R. Kebande, N. M. Karie and H. S. Venter, Adding digital forensic readiness as a security component to the IoT domain, Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 1, pp. 1-11, 2018.

» W. M. S. Stout and V. E. Urias, Challenges to securing the Internet of Things, Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST), pp. 1-8, Oct. 2016.

» Z. A. Solangi, Y. A. Solangi, S. Chandio, M. B. S. A. Aziz, M. S. B. Hamzah and A. Shah, The future of data privacy and security concerns in Internet of Things, Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD), pp. 1-4, May 2018.

» P. S. Shinde and S. B. Ardhapurkar, Cyber security analysis using vulnerability assessment and penetration testing, Proc. World Conf. Futuristic Trends Res. Innov. Social Welfare (Startup Conclave), pp. 1-5, Feb. 2016.

» P. Dholey and A. K. Shaw, OnlineKALI: Online vulnerability scanner, Proc. Int. Ethical Hacking Conf. Adv. Intell. Syst. Comput., vol. 811, pp. 25-35, 2019.

» P. Russo, A. Caponi, M. Leuti and G. Bianchi, A web platform for integrated vulnerability assessment and cyber risk management, Information, vol. 10, no. 7, pp. 242, Jul. 2019.

» R. Stevens, D. Votipka, E. M. Redmiles, C. Ahern and M. L. Mazurek, Applied digital threat modeling: It works, IEEE Secur. Privacy, vol. 17, no. 4, pp. 35-42, Jul. 2019.

» J. M. Archibald and K. Renaud, Refining the PoinTER â€˜human firewallâ€™ pentesting framework, Inf. Comput. Secur., vol. 26, no. 4, pp. 575-600, 2019.

» B. Woods and A. Bochman, Supply chain in the software era in Scowcroft Center for Strategic and Security, Washington, DC, USA:Atlantic Council, May 2018.

» A. Yeboah-Ofori and F. Katsriku, Cybercrime and risks for cyber physical systems, Int. J. Cyber-Secur. Digit. Forensics, vol. 8, no. 1, pp. 43-57, 2019.

» R. D. Labati, A. Genovese, V. Piuri and F. Scotti, Towards the prediction of renewable energy unbalance in smart grids, Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI), pp. 1-5, Sep. 2018.

» J. Boyens, C. Paulsen, R. Moorthy and N. Bartol, Supply chain risk management practices for federal information systems and organizations, NIST Comput. Sec., vol. 800, no. 161, pp. 32, 2015.

» Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, Gaithersburg, MD, USA, 2018.

» F.-J. Hinojo-Lucena, I. Aznar-Diaz, M.-P. Caceres-Reche, J.-M. Trujillo-Torres and J.-M. Romero-Rodriguez, Factors influencing the development of digital competence in teachers: Analysis of the teaching staff of permanent education centres, IEEE Access, vol. 7, pp. 178744-178752, 2019.

» K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac and T. Zwaans, The human aspects of information security questionnaire (HAIS-Q): Two further validation studies, Comput. Secur., vol. 66, pp. 40-51, May 2017.

» B. D. Sawyer and P. A. Hancock, Hacking the human: The prevalence paradox in cybersecurity, Hum. Factors J. Hum. Factors Ergonom. Soc., vol. 60, pp. 597-609, Aug. 2018.

» B. K. Wiederhold, The role of psychology in enhancing cybersecurity, Cyberpsychol. Behav. Social Netw., vol. 17, no. 3, pp. 131-132, Mar. 2014.

» D. E. de Zafra, S. I. Pitcher, J. D. Tressler, J. B. Ippolito and M. Wilson, Information technology security training requirements?: A role- and performance-based model, 1998.

» N. Sun, J. Zhang, P. Rimba, S. Gao, Y. Xiang and L. Y. Zhang, Data-driven cybersecurity incident prediction: A survey, IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1744-1772, 2nd Quart. 2018.

» S. N. Matheu, J. L. HernÃ¡ndez-Ramos, A. F. Skarmeta and G. Baldini, A survey of cybersecurity certification for the Internet of Things, ACM Comput. Surv., vol. 53, no. 6, pp. 1-36, Nov. 2021.

» D. S. Herrmann, Using the Common Criteria for IT Security Evaluation, Boca Raton, FL, USA:CRC Press, 2002.

» N. Sun, C.-T. Li, H. Chan, B. D. Le, M. Islam, L. Y. Zhang, et al., Defining security requirements with the common criteria: Applications adoptions and challenges, IEEE Access, vol. 10, pp. 44756-44777, 2022.

» W. Stallings, L. Brown, M. D. Bauer and A. K. Bhattacharjee, Computer Security: Principles and Practice, Upper Saddle River, NJ, USA:Pearson, 2012.

» K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip and R. Gerdes, Intelligent transportation system security: Impact-oriented risk assessment of in-vehicle networks, IEEE Intell. Transp. Syst. Mag., vol. 13, no. 2, pp. 91-104, May 2021.

» T. T. Dandala, V. Krishnamurthy and R. Alwan, Internet of vehicles (IoV) for traffic management, Proc. Int. Conf. Comput. Commun. Signal Process. (ICCCSP), pp. 1-4, Jan. 2017.

» W. Yanbang, Y. Jing and Y. Zhilou, Auto-driving vehicle testing method ECU and system, 2018.

» H. Pingguo, Y. Jingjing and C. Xiao, Security access control method for vehicle diagnosis system, Jun. 2014.

» R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas and A. Alamoody, An overview on V2P communication system: Architecture and application, Proc. 3rd Int. Conf. Eng. Technol. Appl. (IICETA), pp. 174-178, Sep. 2020.

» A. Vives, Social and environmental responsibility in small and medium enterprises in Latin America, J. Corporate Citizenship, vol. 2006, no. 21, pp. 39-50, Mar. 2006.

» K. Renaud and G. R. S. Weir, Cybersecurity and the unbearability of uncertainty, Proc. Cybersecurity Cyberforensics Conf. (CCC), pp. 137-143, Aug. 2016.

» K. Renaud and G. R. S. Weir, Cybersecurity and the unbearability of uncertainty, Proc. Cybersecurity Cyberforensics Conf. (CCC), pp. 137-143, Aug. 2016.