ISSN No- 2584-2706

Impact of Cyber Security on Network Traffic

Gabriel Tosin Ayodele
Faculty of Engineering and Informatics, University of Bradford,
Bradford West Yorkshire,
United Kingdom.

Abstract
The importance of cybersecurity in safeguarding network traffic is crucial in our increasingly interconnected world. Our research investigates the significant impact of cybersecurity on network performance and integrity, revealing that various security protocols influence the dynamic nature of network traffic in the face of cyber threats. Using data from Kaggle, we conducted an analysis of suspicious activity patterns over time, the contribution of different network protocols, and the involvement of specific IP addresses in attacks. Our findings highlight that cybersecurity incidents notably alter traffic patterns, with peaks often coinciding with increased threat levels. Certain network protocols, such as ICMP and TCP, were identified as key factors influencing traffic and vulnerabilities. Particularly, there was a high frequency of attacks targeting Windows devices, emphasizing the need for specialized security measures.

In the current era, characterized by advancing technologies like IoT and cloud computing, striking a balance between security and performance is a significant concern due to the expanded attack surface area. These results provide valuable insights for developing adaptive and resilient network infrastructures capable of withstanding the evolving landscape of cyber threats.

Keywords
Cybersecurity, Network Traffic, Cyber Threats, Data Integrity, Network Protocols, IP Addresses, Cybersecurity Measures, Real-Time Monitoring, Anomaly Detection, Emerging Technologies.

A. Introduction

In today's interconnected world, the reliance on digital networks for communication, commerce, and vital infrastructure has significantly increased. This growing reliance has also emphasized the importance of robust cybersecurity to safeguard sensitive data and ensure uninterrupted operation of network systems
[1]. Cybersecurity encompasses all practices and protocols aimed at preventing unauthorized access or cyber-attacks on networks, devices, or information. Meanwhile, network traffic encompasses all data transmitted across a network, including activities like web browsing, file transfers, and video streaming. This is crucial for enabling effective communication between devices. Cybersecurity plays a central role in protecting network traffic from various threats, such as malicious attacks, unauthorized system access, and potential compromise of personal or national security, which can greatly impact someone's financial standing and reputation

[2] The impact of cybersecurity on network traffic runs deep and is complex. Because of this, it is essential to have effective security protocols and mechanisms in place to detect, prevent, and mitigate cyber threats targeting the network infrastructure [20]. Cyberattacks like Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), phishing, and ransomware take advantage of weaknesses in network systems, leading to disruption of normal data flow and posing risks to its confidentiality and integrity [3]. Due to their ever-changing nature, these threats require continuous monitoring and adaptive security strategies to uphold the resilience and dependability of network communications.

Furthermore, the implementation of advanced cybersecurity measures impacts the network's performance and effectiveness. Techniques for safeguarding data transmission, such as encryption, Intrusion Detection Systems (IDS), and firewalls, are essential, but they can introduce latency and complexity to network operations [4]. Balancing security and performance to ensure a secure yet efficient network service is an ongoing challenge for organizations. The introduction of

ISSN No- 2584-2706

new technologies like the Internet of Things (IoT) and cloud computing has expanded the attack surface, increased vulnerabilities and adding complexity to the management of secure network traffic.

The study's purpose is to examine the intricate connections between cyber security and network traffic, analyzing various threats and security performance metrics to safeguard network integrity. Using a dataset sourced from Kaggle, the research aims to identify effective methodologies and technologies for network protection while maintaining operational efficiency. It is crucial to gain a deeper understanding of these dynamics to develop robust network systems capable of withstanding and adapting to the constantly evolving landscape of cyber-attacks.

B. Literature Review

The review covers important elements of cybersecurity, including strategies and tools designed to protect valuable information. It also addresses other challenges posed by cybercriminals, such as malware infections and phishing schemes, as well as crucial elements like antivirus software, firewalls, and encryption. Furthermore, it explores the ways in which AI has enhanced network security by offering advanced traffic analysis.

C. Cybersecurity

The concept of cybersecurity encompasses a wide array of methods, strategies, and procedures designed to safeguard data, networks, software, and devices from unauthorized access and attacks [5][6] – [10]. Large volumes of data are often gathered and stored on computers or similar devices by financial institutions and government entities [7][11][12]. Additionally, internet usage plays a crucial role in the operations of sectors like the military and healthcare [7][11][12]. Within these systems, valuable and sensitive items, such as personal identification records, financial documents, and intellectual property, are frequently stored, necessitating the implementation of strict access controls due to the severe repercussions of unauthorized access [11][12]. Consequently, these organizations must implement cybersecurity measures [11] – [14] to mitigate potential risks.

During business transactions, devices exchange sensitive information over networks, making data protection essential at every stage of its life cycle [15]-[18]. Organizations responsible for managing financial records, health care information, and national security data are significantly obligated to implement highly stringent measures to safeguard their sensitive business and personnel records from increasingly sophisticated and frequent cyber-attacks [15][16][17][18]. A solid cyber security policy will effectively incorporate security mechanisms to thwart malicious attacks that seek to access, alter, or delete sensitive information or disrupt systems [19][20][21]. Additionally, cyber security measures can also act as a defense against attacks that could cripple or disrupt devices and systems [19].

D. Cybercriminals

The term cybercrime refers to any criminal activities carried out using computers, connected devices, or networks [22]– [26]. Most cybercrimes are motivated by personal gain, while others aim to disrupt systems or hinder productivity. Examples include using a computer or network to spread malware or distribute explicit content online [22]-[26]. The Council of Europe Convention on Cybercrime covers a wide range of malicious activities, such as illegal data interception, copyright infringement, and compromising network integrity and availability through system intrusions [27][28]. The United States, along with other countries, will be signing this convention [27] [28].

Due to the availability of reliable internet connections, criminals find it simpler to engage in cybercrimes without needing to be physically present [29]. Examples of these offenses include fraud, money laundering, cyberbullying, and cyberstalking, all facilitated by the speed and convenience of the internet [15][19][28][29]. This type of crime may be committed by individuals or organized global criminal groups with advanced technical skills. Additionally, cybercriminals often reside in regions with inadequate laws against such activities, allowing them to operate without detection or arrest [30][31].

E. Cyber Attacks

The individual or organization clearly made a deliberate and sophisticated attempt to disrupt other people's computer systems [32]. While many

ISSN No- 2584-2706

attacks are motivated by financial gain, some seek to delete, alter, or destroy data [5][7][31][32]. Cyber-attacks are now more common. According to the Cisco Annual Cybersecurity Report, attackers can now launch their campaigns using network-based ransomware worms without human intervention [33]. Additionally, security incidents have become both more frequent and more complex [33]. According to the former CEO of Cisco, businesses can be divided into those that have already been hacked and those that are still unaware of any hacking activity [34].

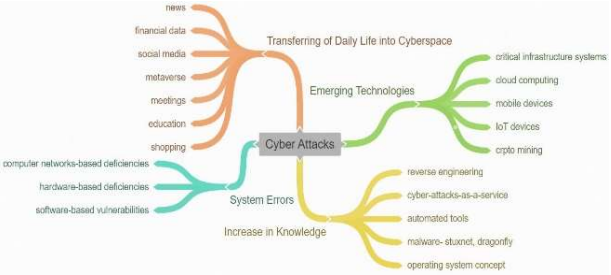


Figure 1: Primary Motivations Behind Cyber-Attacks.

The indications of malicious attacks on computer systems can be observed in six main ways: malware, phishing, denial of service (DoS), man-in-the-middle (MitM), password spraying, and cross-site scripting (XSS) [32] – [41]. The following provides a brief description of each type:

1) Malware: Malware consists of damaging software or code designed to compromise the confidentiality, integrity, or availability of information [42]. It encompasses various types such as Trojans, viruses, worms, spyware, and ransomware [32][35][42].

- Trojans: Trojans masquerade as legitimate software, tricking users into easily installing them and providing cybercriminals an opportunity to steal data [35][43].
- Viruses: Viruses replicate themselves and spread through systems, infecting files or attaching themselves to executable codes [32][43][44].
- Worms: Worms are self-replicating applications that travel through networks, leading to denial-of-service attacks [35][43][45].
- Spyware: Spyware gathers information about the user, including browsing behaviors and personal information, often sent back to attackers [32][35][43][46].
- Ransomware: Ransomware is a type of malware that restricts user access until payment is made, usually by encrypting the victim's documents and holding them hostage [32][35][47][48].

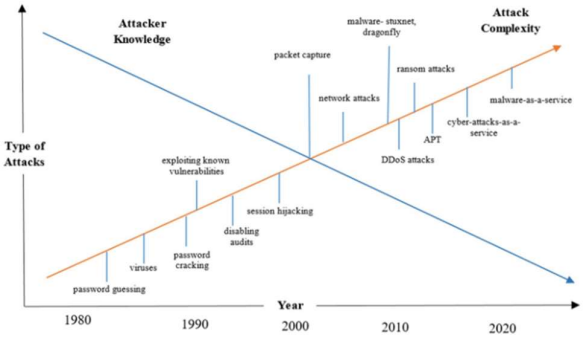


Figure 2: Correlation Between Attackers' Technical Expertise and the Complexity of Attacks.

2) Phishing: Phishing involves sending fake emails that appear genuine, directing recipients to malicious websites or files where attackers can steal sensitive data like logins, credentials, and financial information from their targets.

3) Denial of Service (DoS) and Distributed Denial of Service (DDoS): Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks overwhelm systems with traffic, rendering them unable to respond to legitimate requests. DDoS attacks, in particular, are challenging to prevent as they involve multiple computers simultaneously.

4) Man-in-the-Middle (MitM): In a Man-in-the-Middle (MitM) attack, hackers intercept communication between clients and servers by impersonating either party, gaining access to sensitive information.

5) Brute-force and Password Spraying: Brute-force attacks involve repeatedly guessing passwords until one is successful, while password spraying involves bypassing lockout protocols by trying common passwords across multiple accounts.

6) Cross-site Scripting (XSS): Cross-site Scripting (XSS) exploits vulnerabilities in web applications, allowing hackers to inject malicious code into websites to collect user data without their consent.

F. Cybersecurity Tools and Techniques in Network Security and Traffic Analysis

Unauthorized attempts to access confidential information have significantly increased in the current scenario. These attempts often involve stealing data or manipulating sensitive information to influence users. This growing threat emphasizes the crucial need for prioritizing cybersecurity measures [5][6][7][8][9]. Internet security can be achieved using antivirus programs, firewalls, authentication methods, encryption technologies, and digital signatures, each of which will be discussed below.

- Anti-Virus: An undesirable program that executes commands without user approval is known as a computer virus. The primary functions of an anti-virus tool are to prevent virus installations and to scan systems for potential viruses [7][49]. While Windows operating systems are the primary targets for viruses due to their widespread usage, some viruses also target Apple and Linux platforms [49][50].
- Firewall: Firewalls act as barriers against hackers attempting to infiltrate a system through internet or other network connections [57][58]. Most operating systems come with built-in firewalls that are typically activated by default. However, users can opt to install additional commercial firewalls if the default ones do not offer sufficient protection or disrupt legitimate network activities [57][58].
- Authentication: Verifying credentials is a crucial cybersecurity concept aimed at ensuring that users' identities match the information in the system's security domain [59]. Passwords are a primary authentication tool, and other methods such as SIM cards with unique ID numbers are also utilized. During the authentication process, these numbers are transmitted over a secure line [59]– [60]. However, intercepting passwords through unprotected channels is a significant challenge, which can be addressed by implementing encrypted techniques [59]– [60].
- Encryption: Encryption involves converting data into an unreadable format to ensure that only authorized individuals can access it using the correct keys. Breaking into encrypted information typically involves solving complex mathematical tasks such as factoring large primes, which requires a considerable amount of time and resources [61][62]. There are two main types of cryptographic standards: symmetric and asymmetric. Symmetric encryption relies on a single key for both encoding and decoding, while the asymmetrical method uses public/private keys. Furthermore, modern security protocols often utilize asymmetric encryption to securely distribute keys [61].
- Digital Signatures: The same mathematical principles underpin digital signatures and asymmetric encryption [63]. Users can verify their ownership of a specific private key by using encoded information. The user's public key is used for decryption and verification of their credentials. This process utilizes public key encryption and rests on the assumption that only the authorized user has access to the private key [63] [64].
- AI-Driven Network Traffic Analysis: AI-powered analysis of network traffic has revolutionized the monitoring and analysis of network activity. Specifically, deep learning models have automated the detection of abnormalities and security threats within network traffic (AI). These systems facilitate the classification and monitoring of traffic patterns, as well as the detection of anomalies and the enhancement of intrusion detection, among other functions. Within these networks, deep learning models such as CNNs or RNNs have demonstrated significant potential in identifying malicious traffic across intricate networks. This technique plays a crucial role in ensuring robust network security.

G. Methodology

The research provided an analysis of the impact of computer security breaches on network communications through data preparation and visual exploration. Specifically, the data was cleansed and structured to facilitate an investigation aimed at distinguishing between normal and malicious traffic. Utilizing Plotly, interactive visualizations were generated, aiding

ISSN No- 2584-2706

in the identification of patterns, anomalies, and threat assessments. This approach allowed for a comprehensive understanding of network activities during cyberattacks.

H. Dataset

The study utilizes a dataset obtained from Kaggle, containing 40000 rows and 25 columns. It comprises network traffic data such as timestamps, source and destination IP addresses, and various traffic-related components. This dataset encompasses diverse types of network activities and potential security events, including network intrusions, anomalies, and attack patterns.

Source Port	Destination Port	Protocol	Packet Length	Packet Type	Traffic Type	Payload Data	...	Browser	Device/OS	Year	Month	Day	Hour	Minute	Second	DayOfWeek
31225	17616	ICMP	503	Data	HTTP	Qui natus odio asperiores nam. Optio nobis ius...	...	Mozilla	Windows	2023	5	30	6	33	58	Tuesday
17245	48166	ICMP	1174	Data	HTTP	Aperiam quos modi officiis veritatis rem. Omni...	...	Mozilla	Windows	2020	8	26	7	8	30	Wednesday
16811	53600	UDP	306	Control	HTTP	Perferendis sapiente vitae soluta. Hic delectu...	...	Mozilla	Windows	2022	11	13	8	23	25	Sunday
20018	32534	UDP	385	Data	HTTP	Totam maxime beatae expedita explicabo porro l...	...	Mozilla	Macintosh	2023	7	2	10	38	46	Sunday

Figure 3: Dataset Overview

I. Data Preprocessing

To ensure the dataset was clean and suitable for analysis, the following preprocessing steps were performed:

- Handling Missing Values: Any rows with missing or null values were removed to prevent inaccuracies in the analysis.

```
In [8]: # Determine recent activity
df['Alerts/Warnings'] = df['Alerts/Warnings'].apply(lambda x: 'yes' if x == 'Alert Triggered' else 'no')

df['Proxy Information'] = df['Proxy Information'].apply(lambda x: 'No proxy' if pd.isna(x) else x)

df['Malware Indicators'] = df['Malware Indicators'].apply(lambda x: 'No Detection' if pd.isna(x) else x)

df['Firewall Logs'] = df['Firewall Logs'].apply(lambda x: 'No Data' if pd.isna(x) else x)

df['IDS/IPS Alerts'] = df['IDS/IPS Alerts'].apply(lambda x: 'No Data' if pd.isna(x) else x)

df.isnull().sum().sort_values(ascending=False)
```

Figure 4: Code Snippet for Handling Missing Value

- Data Type Conversion: The timestamp column was converted into a standard datetime format to ensure time-based analysis was consistent and accurate.

```
In [12]: def extract_time_features(df, Timestamp):
             df[Timestamp] = pd.to_datetime(df[Timestamp])

             # Extract time features
             df['Year'] = df[Timestamp].dt.year
             df['Month'] = df[Timestamp].dt.month
             df['Day'] = df[Timestamp].dt.day
             df['Hour'] = df[Timestamp].dt.hour
             df['Minute'] = df[Timestamp].dt.minute
             df['Second'] = df[Timestamp].dt.second
             df['DayOfWeek'] = df[Timestamp].dt.dayofweek

             return df
```

Figure 5:Code Snippet for Data Type Conversion

- Labeling Network Traffic: Traffic was categorized based on whether it represented normal activity or potential attacks, allowing for a clear distinction in the analysis of benign versus malicious traffic.

J. Analysis

The study utilized data visualizations to tackle the primary research inquiries, aiming to explore the impact of cybersecurity events on network traffic patterns. Rather than using machine learning models for prediction or classification, the emphasis was on deriving insights from the dataset by generating visual depictions of network activities.

Key steps in the analysis process included:

- Identifying Core Questions: The analysis was guided by several key questions to comprehend the impact of cyber security on data traffic. The objective was to determine the disparity in network traffic from specific addresses compared to others, as well as to identify prevalent types of attacks. Equally important was examining the duration of different types of connections and identifying any substantial increases during periods associated with cyber-crimes. By addressing these queries, the study aimed to uncover significant patterns and anomalies in the network that could signal potential security threats.
- Data Exploration Through Visualizations: I utilized a series of charts and graphs to delve into key research questions and gain a deeper understanding of the data. Each visualization was tailored to emphasize specific aspects of network traffic, shedding light on metrics such as traffic volume, types of attacks, and time-based trends. By employing scatter plots and heatmaps, I was able to illustrate the flow of network traffic and identify which IP addresses were more likely to be associated with abnormal traffic during cyber-attacks. Dedicated graphs provided valuable insights into whether malicious activity was correlated with shorter or longer connection times when examining connection duration. Additionally, bar charts and pie charts were used to showcase the distribution of different types of attacks, helping to pinpoint more severe threats facing the network.
- Investigating Time Variability Patterns: Specifically, line charts proved to be effective in examining fluctuations in network traffic over time. By plotting time values against traffic volume, we were able to detect unusual peaks or trends in network activity which often correlated with cybersecurity incidents. Through this temporal analysis, we were able to identify peak vulnerability moments and significant cyber activities.
- Bringing Attention to Emerging Abnormalities: We utilized scatter plots and heat maps to highlight anomalies such as unusual traffic spikes, as well as the presence of outlier connections, among other things. These visual tools simplified the identification of behaviors that signal attacks on computers or other suspicious activities on the internet, as they

clearly illustrate the distinct patterns associated with these behaviors.

- A Visual Representation Is Invaluable: The study was able to draw important conclusions about how network dynamics changed in relation to cybersecurity events by exclusively relying on visual exploration of the available data. A visual approach allows for nonverbal comprehension of complex information, making it easier to detect trends and anomalies that traditional statistical methods may overlook.
- Iterative Process: Through an iterative process, new insights were uncovered by repeatedly visualizing the data, allowing for a more in-depth exploration. When new patterns or anomalies arose, additional visualizations were created to delve into specific findings.

  By honing in on these crucial questions using visuals, the research thoroughly examined network traffic and its vulnerabilities to cyber security incidents. This method offered a detailed yet user-friendly way to demonstrate how network behaviors changed in response to security threats, enabling recommendations for enhancing network monitoring and threat detection mechanisms.

K. Visualization Tools

In this study on the impact of cybersecurity incidents on network traffic, the investigation relied on Plotly, an interactive and powerful data visualization library. Plotly was chosen for its ability to create adaptable and interactive charts, enabling in-depth analysis of network traffic patterns.

- Interactive Visualizations: Plotly's primary advantage lies in its ability to generate interactive plots. It offers features such as zooming in on specific areas, accessing more information by hovering over data points, and dynamically filtering or adjusting the view. These capabilities proved particularly helpful in comprehending complex network traffic patterns, where detecting specific anomalies or trends necessitated thorough exploration.
- Plot Types: Various chart types were utilized to provide insights into different aspects of the dataset:
-

  Scatter Plots: These plots were used to display the relationship between features like Source IP Address, Destination IP Address, and Connection Duration, allowing visualization of normal traffic clusters and potential outliers indicating suspicious behavior.
  Line Charts: Utilized to showcase variations in network traffic over time. This enabled the identification of spikes or unusual patterns that could be indicative of cyber-attacks.
  Bar Charts: Bar Charts are employed to compare the frequency of different types of network traffic, such as normal versus attack traffic, to analyze the distribution of various attacks.
  Heatmaps are utilized to visualize the concentration of network traffic between specific source and destination IP addresses, thereby identifying potentially anomalous connections.

- Plotly offers customization options to enhance the clarity and presentation of each graph's different elements. Therefore, customizations were implemented, including clear and descriptive labeling of the x-axis and y-axis to ensure easy comprehension.

  Distinct color schemes are used to differentiate normal traffic from potential attacks. For example, cyber-attacks are highlighted in red, while normal traffic is depicted in green or blue.

  Annotations are added to highlight key events, such as periods of increased network activity or suspected attacks, on the plots to showcase important findings.

- Interactive Live Data: Plotly images can be accessed on web platforms, offering the advantage of real-time interactivity. This enables continuous monitoring of network traffic patterns. Even though the analysis was based on a static dataset, these tools have the potential to be used in real time for network

monitoring and quick anomaly detection, contributing to better network administration.

L. Results and Discussion

In this section, we examine various aspects of cyber threats, including the timing of suspicious activities, the impact of transport protocols on internet traffic vulnerability, and the significance of IP addresses in cyber-attacks. Our analysis covers the influence of different protocols on packet size and security, as well as common threats associated with major IPs and the specific vulnerabilities of devices using Windows, which are frequently targeted. Furthermore, we investigate the potential use of log sources for detecting and responding to threats, and provide suggestions for improving security measures and response strategies.

M. Time Patterns of Suspicious Network Activities

It is important to investigate patterns of abnormal network behavior over time in order to identify high-risk periods and enhance cybersecurity. Organizations can analyze year-on-year, month-on-month, day-on-day, and hourly data to allocate resources wisely and anticipate potential attacks during periods of heightened risk.

An analysis of data from 2020 to 2023 shows a consistent number of incidents, with over 10,000 suspicious actions reported each year until 2023, when a decrease to 8139 was observed. This decrease may indicate improvements in security measures or shifts in attack patterns.

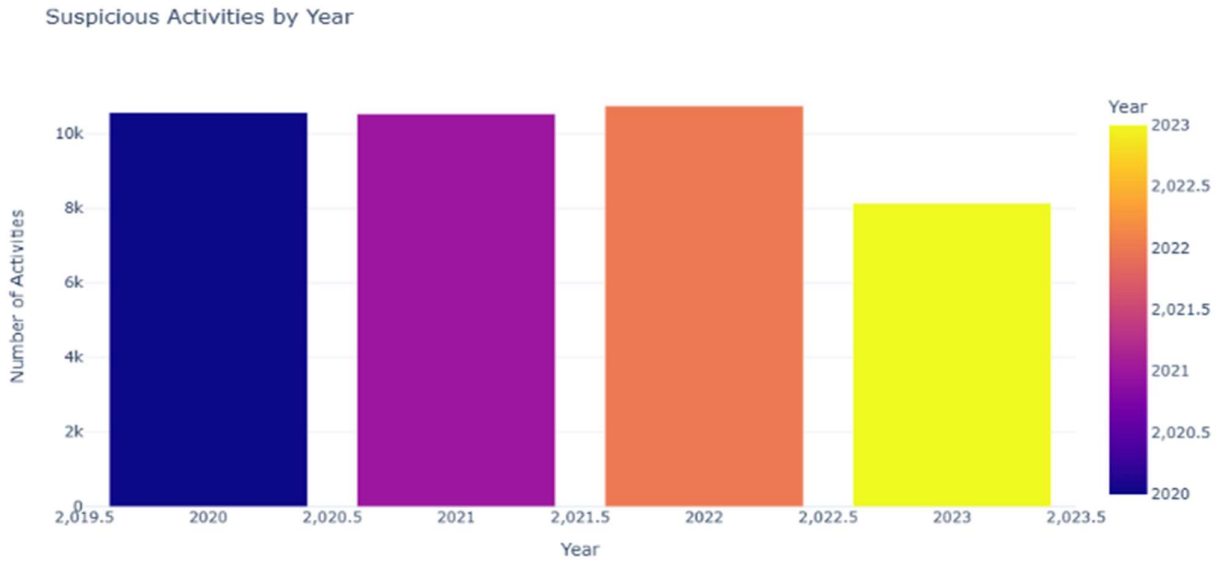


Figure 6: Plot of Network Yearly Patterns

Some months, such as December 2020, June 2021, and July 2022, experienced high levels of activity. Analysis of monthly trends demonstrates variations, suggesting that attackers may be taking advantage of less secure periods for organizations.

ISSN No- 2584-2706

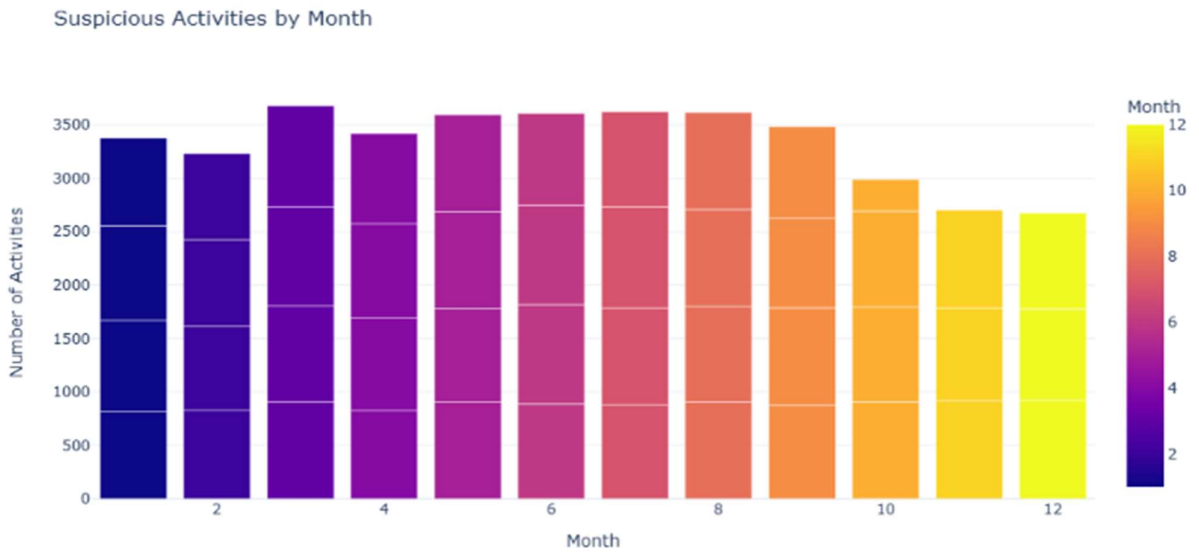


Figure 7: Plot of Network Monthly Patterns

When looking at the days of the week, it is evident that there is increased activity on weekdays, with Fridays being particularly susceptible to incidents. This pattern implies that attackers tend to focus on busy days when security measures may be more relaxed within organizations.

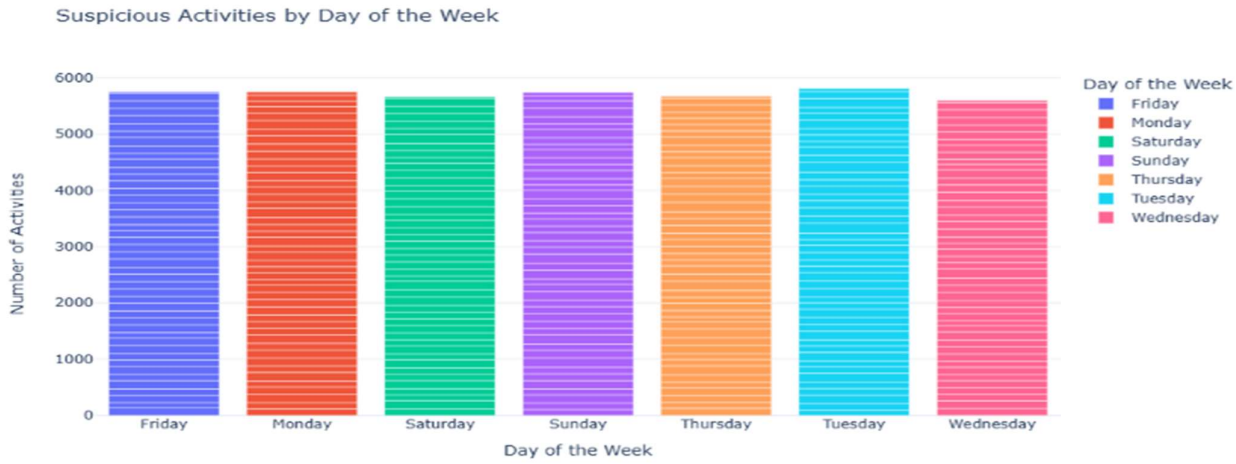


Figure 8: Plot of Network Weekly Patterns

As a result, it is essential for organizations to continuously monitor and adapt their cybersecurity strategies based on these temporal patterns. They should also strengthen their defense mechanisms, especially during peak periods like busy days or months, to mitigate potential cyber-attacks. This can be achieved by anticipating and reducing response times, as well as minimizing the likelihood of similar incidents occurring in the future.

N. Impact of Protocols on Packet Length and Traffic Type

Protocols such as ICMP, TCP, and UDP play a crucial role in understanding the behavior of different types of traffic and the potential impact of large packets, especially in security-sensitive environments. Analyzing the average, maximum, and minimum packet lengths across various traffic

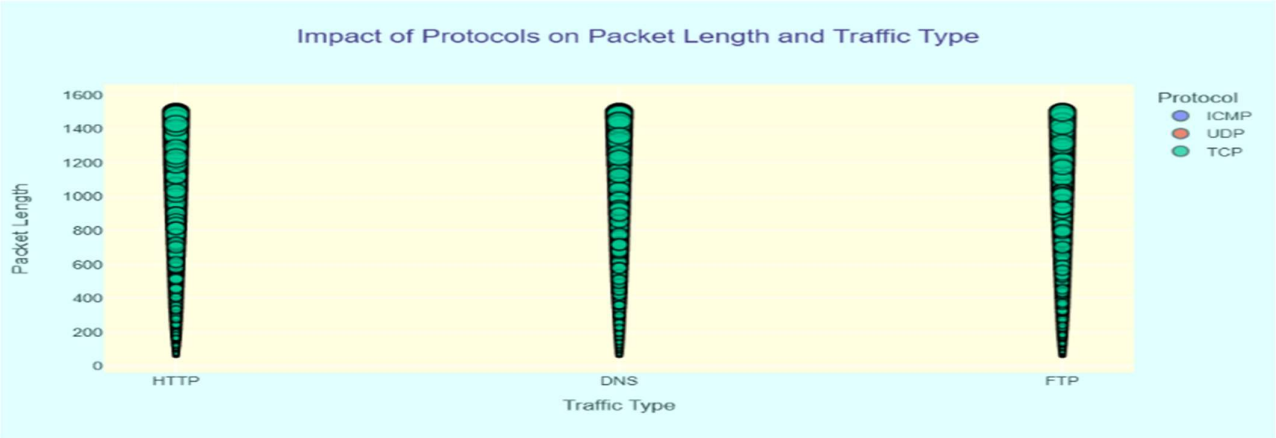
ISSN No- 2584-2706

types including DNS, FTP, and HTTP allows us to dive into the behavior of these protocols.

The findings reveal that ICMP tends to have slightly larger mean packet lengths compared to TCP and UDP. Across all protocols, the maximum packet length can reach up to 1500 bytes. This signifies that ICMP, commonly utilized for error messages and diagnostics, frequently handles larger packets, potentially leading to increased data volume during large-scale detection or ping operations. TCP, known for reliable connection-based communication, maintains nearly consistent packet sizes, emphasizing its role in ensuring precise data transmission, essential for traffics like FTP or HTTP. Conversely, UDP, a non-

connection oriented and faster transmission approach, maintains similar mean packet lengths, indicating that speed compromise's reliability without significantly affecting packet size.

Figure 9:Plot Showing the Impact of Protocol



Different protocols handle traffic, which can result in security vulnerabilities. Attackers can exploit the diagnostic nature of ICMP for network reconnaissance, and connection-based TCP can be vulnerable to denial-of-service attacks. UDP's lightweight approach may expose the entire network to amplification attacks. It is crucial to understand this in order to optimize the adoption of security measures in networks and ensure sufficient protection against these vulnerabilities.

Figure 10: Plot Showing Packet Length Across Traffic Type and Protocols

O. Impact of Top IP Addresses on Malicious Traffic and Associated Attack Types

An in-depth investigation into the suspicious traffic reveals that various IP addresses are repeatedly involved in different forms of attacks. The most prevalent among these is the occurrence of malware attacks originating from several prominent source IP addresses, including 103.216.15.12, 197.184.240.174, and 40.119.100.114. Similarly, intrusion attempts on other identified IPs like 119.183.250.156 and 147.178.224.232 are also notable, and there have

ISSN No- 2584-2706

been observed DDoS attempts from 74.225.47.66 and 80.60.140.131. On the other hand, high-ranking destination addresses primarily indicate intrusion or malware occurrences on IPs such as 112.135.140.167 and 14.172.223.72, while DDoS attacks have been witnessed multiple times on addresses like 12525219110 or 20213243236. This highlights the need for specific preventive actions targeted at these types of threats, given the common attack patterns observed.

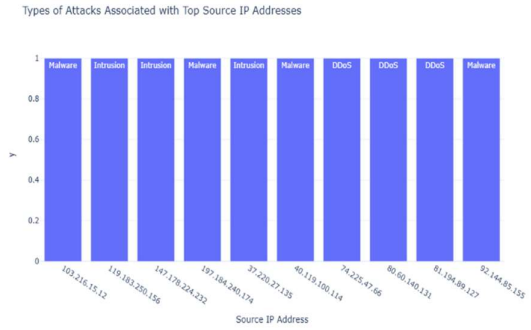


Figure 11: Plot Showing Top IP Sources Based on Attack Types

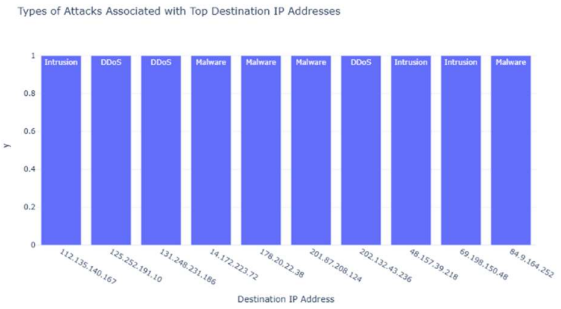


Figure 12: Plot Showing Top IP Destination Based on Attack Types

P. Impact of Packet Length on Threat Types and Device/OS Distribution

The investigation offers intriguing insights into the different threats targeting various devices and operating systems, based on packet length and their average severity.

In terms of total detected threats, Windows is the most targeted platform, with 17,953 threats, followed by Linux with 8,840, Macintosh with 5,813, and iPod with 2,656. iPhone, iPad, and Android have fewer threats, with 1,567, 1,551, and 1,620 instances respectively.

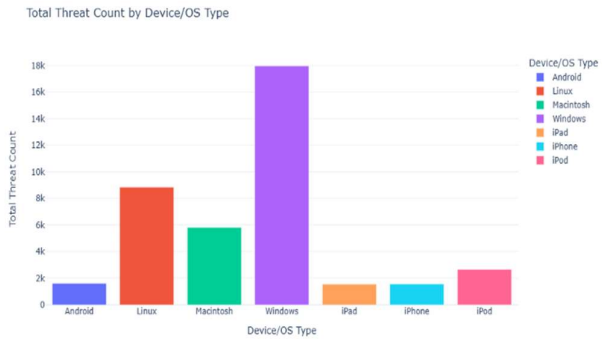


Figure 13: Plot Showing Total Threat by Device

When it comes to the distribution of threat types across different devices and operating systems, Windows faces the highest number of threats across all attack categories, including DDoS, Intrusion, and Malware. On the other hand, Linux and Macintosh have significantly fewer threats across these categories compared to Windows. The distribution illustrates that DDoS and malware target Windows the most, while other operating systems, like iPad, have minimal threats in comparison.

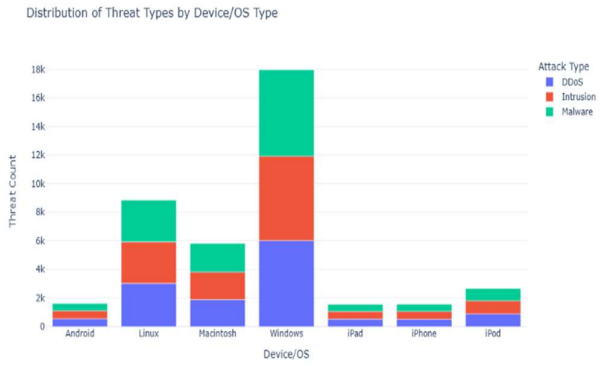


Figure 14: Plot Showing Distribution of Threat by Device

The average length of packets can provide insight into the severity of threats and slightly differs across devices. iPads stand out with an average packet length of 800.30 bytes, indicating the potential for more severe threats or larger data transfers. On the other hand, android devices have a lower average packet length of 786.72 bytes but still face a significant number of attacks. Windows, Macintosh, and iPod have similar average packet lengths, suggesting that they experience threats with similar intensity.

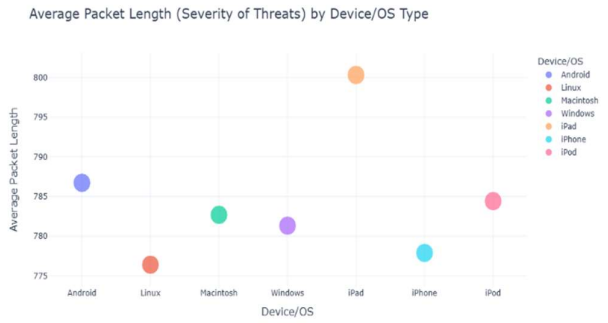


Figure 15: Plot Showing Severity of Threat by Device

Furthermore, these findings suggest that Windows is the most targeted device type with various attack vectors and significant threat impact. Therefore, understanding the reasons for variations in packet length among different devices can help identify the types of threats and their implications on these platforms, guiding focused security efforts and responses.

Q. Analysis of Threat Detection and Response Time

Analysis of threat detection trends from multiple log sources has uncovered some intriguing patterns. Specifically, the Firewall log source has been instrumental in combating numerous threats, with 6,734 DDoS attacks, 6,638 intrusion attempts, and 6,744 malware incidents detected. This underscores its crucial role in monitoring and addressing various threat types. Conversely, the Server log source has recorded 6,694 DDoS attacks, 6,627 intrusion attempts, and 6,563 malware incidents, indicating a nearly equal capacity to detect different threat types, albeit with slightly lower numbers for malware. While both log sources are effective, the Firewall demonstrates a marginally higher detection rate for specific threats.

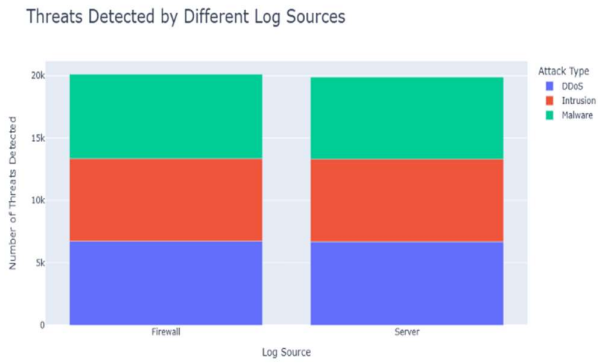


Figure 16: Plot Showing Threats by Log Sources

The average response times show some anomalies. DDoS attacks have an average response time of -981,523.56s, Intrusions at 26,535.96s, and Malware incidents at -391,837.36s on the Firewall. Meanwhile, on the Server, DDoS attacks have an average response time of 984,308.56 seconds, Intrusions at -23,444.39s, and Malware infections at 404,225.89s. The negative values raise concerns about the accuracy of time stamps, potentially indicating inconsistencies or errors during the recording process. Despite the vital roles played by Firewalls and Servers in detecting network threats, the significant data quality problems suggested by their average response times warrant further extensive investigation.

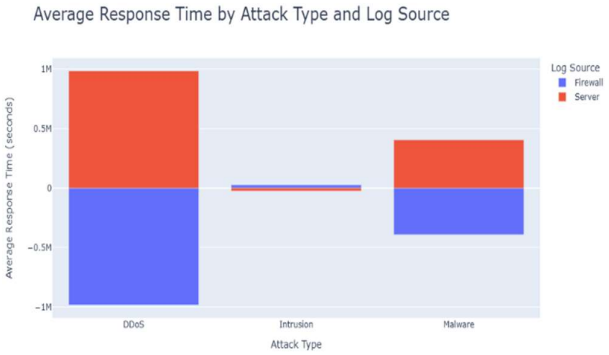


Figure 17: Plot Showing ART by Attack Type and Log

R. Interpretation of Log Source Distribution:

Different types of approaches such as Blocked, Ignored, and Logged are used to counter various attacks including DDoS, Intrusion, and Malware in the log source distribution. It is recommended to adopt a proactive defense strategy. The data indicates that the highest number of threats were

ISSN No- 2584-2706

blocked, with Intrusion leading at 4,553, followed by DDoS at 4,533 and malware at 4,443. However, this could suggest that these threats might be less serious or misclassified. Some attacks were ignored, especially DDoS at 4,459, Intrusion at 4,401, and Malware at 4,416. There was a balanced logging activity for all attack types, with Malware having slightly more records at 4,448 compared to DDoS (4,436) and Intrusion (4,311). This suggests a greater focus on blocking, while logging and ignoring attacks can sometimes suffice for monitoring purposes.

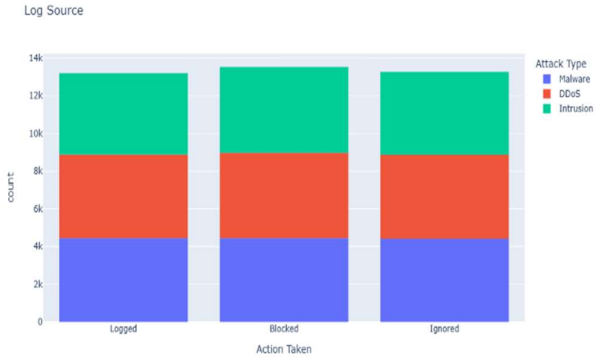


Figure 18: Plot Showing Log Source by Attack Type

- **Conclusion And Recommendation**

The analysis of cybersecurity's impact on network traffic has revealed the complex and diverse ways in which security measures influence network behavior. By examining time patterns of suspicious activities, the influence of network protocols, the involvement of IP addresses in attacks, and the distribution of threats across devices and operating systems, we have gained insight into how computer threats impact network movements.

Our research indicates a strong correlation between cybersecurity incidents and changes in network traffic behavior, particularly during peak times when there is a higher prevalence of such threats. We have established that different protocols such as ICMP, TCP, or UDP have distinct roles in transmitting data packets and their associated vulnerabilities. It is evident that frequently targeted IP addresses highlight common methods that hackers use to access systems, necessitating specific countermeasures against these threats. Furthermore, the majority of attacks were aimed at Windows devices, underscoring the importance of implementing tailored security strategies across different platforms for effective protection.

In addition, an examination of traffic volume over time has revealed a correlation between peak traffic periods and spikes in security incidents. This underscores the need for continuous monitoring and adaptable security measures to prevent potential risks. Tools and methods such as firewalls, encryption, and AI-based traffic analysis have proven effective in addressing these threats by providing protection against them.

To enhance network security effectively, we propose the following:

- Implement Real-time Monitoring: Utilize advanced real-time monitoring systems capable of promptly detecting any abnormal spikes or suspicious activities. The use of AI-powered tools will improve anomaly detection capability, leading to quicker and more precise defense mechanisms.
- Strengthen Protocol-Specific Defenses: Develop specific security measures tailored to different network protocols used by various websites. For example, implementing targeted ICMP protection or TCP protections can help mitigate certain vulnerabilities, thereby reducing potential attack vectors.
- Prioritize testing on insecure IP addresses that are frequently targeted for security breaches. Monitoring and defending these high-risk addresses with threat intelligence can prevent successful breaches and mitigate associated risks.
- Adjust security strategies for different platforms depending on their vulnerabilities. Given that Windows devices are commonly targeted, tailor security measures accordingly and ensure regular updates and patches to protect against known exploits.
- Continuously assess and upgrade cybersecurity tools to keep them current. This includes enhancing encryption methods, digital signatures, and other security features to minimize data protection threats.

- **References**

[1] Abdel-Rahman, M., 2023. Advanced cybersecurity measures in IT service

operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 7(1), pp.138-158.

[2] Mallick, M.A.I. and Nath, R., 2024. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News, 190(1), pp.1-69.

[3] Iftikhar, S., 2024. Cyberterrorism as a global threat: a review on repercussions and countermeasures. Peerj Computer Science, 10, p.e1772.

[4] Al Naim, A.F. and Ghouri, A.M., 2023. Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-commerce Platforms. International Journal of ebusiness and egovernment Studies, 15(1), pp.44-469.

[5] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

[6] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," Materials Today: Proceedings, 2021.

[7] A. Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al- Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," Solid State Technology, vol. 63, no. 5, pp. 7894– 7899, 2020.

[8] S. Cheung, U. Lindqvist, and M. W. Fong, "Modeling multistep cyber attacks for scenario recognition," in Proceedings DARPA Information Survivability Conference And Exposition, vol. 1. IEEE, 2003, pp. 284– 292.

[9] I. Frank and E. Odunayo, "Approach to cyber security issues in nigeria: challenges and solution," International Journal of Cognitive Research in science, engineering and education, vol. 1, no. 1, pp. 100–110, 2013.

[10] P. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber se- curity," International Journal of Advanced Research in Computer and Communication Engineering, vol. 7, no. 11, pp. 125–128, 2018.

[11] C. O. K. CLN, E. I. C.-K. CLN, I. A. A. O. CLN, and B. A. U. CLN, "Issues on information systems, icts, cyber-crimes, cyber security, cyber ethics, and national security in nigeria: Librarians' research," Library Philosophy and Practice, pp. 1–19, 2020.

[12] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, "Using deep learning techniques for network intrusion detection," in 2020 IEEE International Conference on Informatics, iot, and Enabling Technologies (iciot). IEEE, 2020, pp. 171–176.

[13] L. Griffin, "The effectiveness of cybersecurity awareness training in reducing employee negligence within department of defense (dod) affiliated organizations-qualitative exploratory case study," Ph.D. Dissertation, Capella University, 2021.

[14] T. Bhardwaj, H. Upadhyay, and L. Lagos, "Deep learning-based cyber security solutions for smart-city: Application and review," Artificial Intelligence in Industrial Applications, pp. 175–192, 2022.

[15] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," Congressional research service documents, CRS RL32331 (Washington DC), vol. 2, 2004.

[16] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," Computers & Security, vol. 60, pp. 154– 176, 2016.

[17] K. Thakur, M. L. Ali, S. Kopecky, A. Kamruzzaman, and L. Tao, "Connectivity, traffic flow and applied statistics in cyber security," in 2016 IEEE International Conference on Smart Cloud (smartcloud). IEEE, 2016, pp. 295–300.

[18] S. Demirkan, I. Demirkan, and A. Mckee, "Blockchain technology in the future of business cyber security and accounting," Journal of Management Analytics, vol. 7, no. 2, pp. 189–208, 2020.

[19] W. Steingartner, D. Galinec, and A. Kozina, "Threat defense: Cyber deception

approach and education for resilience in hybrid threats model," Symmetry, vol. 13, no. 4, p. 597, 2021.

[20] Kodete, Chandra Shikhi, Bharadwaj Thuraka, Vikram Pasupuleti, and Saiteja Malisetty. 2024. "Determining the Efficacy of Machine Learning Strategies in Quelling Cyber Security Threats: Evidence from Selected Literatures". *Asian Journal of Research in Computer Science* 17 (8):24-33. Https://doi.org/10.9734/ajrcos/2024/v17i7487.

[21] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for california's smart inverter functions," in 2019 IEEE cyberpels (cyberpels). IEEE, 2019, pp. 1–5.

[22] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," Computers in Industry, vol. 103, pp. 97–110, 2018.

[23] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," IEEE Access, vol. 8, pp. 137 293–137 311, 2020.

[24] N. Setiawan, V. C. E. Tarigan, P. B. Sari, Y. Rossanty, M. Nasution, and I. Siregar, "Impact of cybercrime in e-business and trust," Int. J. Civ. Eng. Technol, vol. 9, no. 7, pp. 652–656, 2018.

[25] T. Holt and A. Bossler, Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge, 2015.

[26] R. Anderson, C. Barton, R. Bo¨hme, R. Clayton, M. J. Van Eeten,

[27] M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in The economics of information security and privacy. Springer, 2013, pp. 265–300.

[28] S. Gordon and R. Ford, "On the definition and classification of cybercrime," Journal in computer virology, vol. 2, no. 1, pp. 13–20, 2006.

[29] A. C. Moise et al., "A few comments on the council of europe convention on cybercrime," Jurnalul de Drept si Stiinte Administrative, vol. 2, no. 8, pp. 28–38, 2017.

[30] N. C. Hampson, "Hacktivism: A new breed of protest in a networked world," BC Int'l & Comp. L. Rev., vol. 35, p. 511, 2012.

[31] T. U. Rehman, "Psychosocial aspects of cybercrime victimization in pakistan," in Handbook of Research on Applied Social Psychology in Multiculturalism. IGI Global, 2021, pp. 192–211.

[32] D. Shivpuri, "Cyber crime: Are the law outdated for this type of crime," International Journal of Research in Engineering, Science and Management, vol. 4, no. 7, pp. 44–49, 2021.

[33] A. Sarmah, R. Sarmah, and A. J. Baruah, "A brief study on cyber crime and cyber law's of india," International Research Journal of Engineering and Technology (IRJET), vol. 4, no. 6, pp. 1633–1640, 2017.

[34] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, pp. 65–88, 2015.

[35] C. Ventures, "2019 official annual cybercrime report," in Recuperado el. Herjavec Group, 2019.

[36] R. Fisher, C. Porod, and S. Peterson, "Motivating employees and organizations to adopt a cybersecurity-focused culture," Journal of Organizational Psychology, vol. 21, no. 1, pp. 114–131, 2021.

[37] A. Al-Marghilani, "Comprehensive analysis of iot malware evasion techniques," Engineering, Technology & Applied Science Research, vol. 11, no. 4, pp. 7495–7500, 2021.

[38] A. Goel, D. K. Sharma, and K. D. Gupta, "Leobat: Lightweight encryption and otp based authentication technique for securing iot networks," Expert Systems, vol. 39, no. 5, p. E12788, 2022.

[39] Y. E. Suzuki and S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," Security Journal, vol. 35, no. 4, pp. 1162–1182, 2022.

[40] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges,"

Neural Computing and Applications, vol. 28, no. 12, pp. 3629–3654, 2017.

[41] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

[42] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, "Dos and ddos attacks: defense, detection and traceback mechanisms-a survey," Global Journal of Computer Science and Technology, 2014.

[43] S. Shalini and S. Usha, "Prevention of cross-site scripting attacks (xss) on web applications in the client side," International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, p. 650, 2011.

[44] M. Souppaya, K. Scarfone et al., "Guide to malware incident prevention and handling for desktops and laptops," NIST Special Publication, vol. 800, p. 83, 2013.

[45] A. Sheikh, "Trojans, backdoors, viruses, and worms," in Certified Ethical Hacker (CEH) Preparation Guide. Springer, 2021, pp. 49– 69.

[46] S. Sharma, "Design and implementation of malware detection scheme." International Journal of Computer Network & Information Security, vol. 10, no. 8, 2018.

[47] M. Rai and H. Mandoria, "A study on cyber crimes cyber criminals and major security breaches," Int. Res. J. Eng. Technol., vol. 6, no. 7, pp. 1–8, 2019.

[48] B. Narwal, A. K. Mohapatra, and K. A. Usmani, "Towards a taxonomy of cyber threats against target applications," Journal of Statistics and Management Systems, vol. 22, no. 2, pp. 301–325, 2019.

[49] I. A. Chesti, M. Humayun, N. U. Sama, and N. Jhanjhi, "Evolution, mitigation, and prevention of ransomware," in 2020 2nd International Conference on Computer and Information Sciences (ICCIS). IEEE, 2020, pp. 1–6.

[50] K. K. Gagneja, "Knowing the ransomware and building defense against it-specific to healthcare institutes," in 2017 Third International Confer- ence on Mobile and Secure Services (mobisecserv). IEEE, 2017, pp. 1–5.

[51] M. Papoutsakis, K. Fysarakis, G. Spanoudakis, S. Ioannidis, and K. Koloutsou, "Towards a collection of security and privacy patterns,"

[52] Applied Sciences, vol. 11, no. 4, p. 1396, 2021.

[53] S. Boonkrong, "Methods and threats of authentication," in Authentica- tion and Access Control. Springer, 2021, pp. 45–70.

[54] A. Kanta, S. Coray, I. Coisel, and M. Scanlon, "How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts," Forensic Science International: Digital Investigation, vol. 37, p. 301186, 2021.

[55] R. Beno and R. Poet, "Hacking passwords that satisfy common pass- word policies: Hacking passwords," in 13th International Conference on Security of Information and Networks, 2020, pp. 1–3.

[56] V. Nithya, S. L. Pandian, and C. Malarvizhi, "A survey on detection and prevention of cross-site scripting attack," International Journal of Security and Its Applications, vol. 9, no. 3, pp. 139–152, 2015.

[57] A. M. K. Alhawamleh, "Web based english placement test system (elpts)," Ph.D. Dissertation, Universiti Utara Malaysia, 2012.

[58] A. Raman, S. Kaushik et al., "A comprehensive study of contemporary tools and techniques in the realm of cyber security," IITM Journal of Management and IT, vol. 7, no. 1, pp. 108–120, 2016.

[59] J. L. Duffany, "Computer security," in Computer and Network Security Essentials. Springer, 2018, pp. 3–20.

[60] K. Kallepalli and U. B. Chaudhry, "Intelligent security: Applying artificial intelligence to detect advanced cyber attacks," in Challenges in the iot and Smart Environments. Springer, 2021, pp. 287–320.

[61] M. Chakraborty and M. Singh, "Introduction to network security technologies," in The" Essence" of Network

Security: An End-to-End Panorama. Springer, 2021, pp. 3–28.

[62] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security chal- lenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020.

[63] R. P. Jover, "Security analysis of sms as a second factor of authentica- tion," Communications of the ACM, vol. 63, no. 12, pp. 46–52, 2020.

[64] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A survey on the cryptographic encryption algorithms," International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, 2017.

[65] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asym- metric key encryption algorithms," in 2017 international conference on engineering and technology (ICET). IEEE, 2017, pp. 1–7.

[66] N. G. Kumar and K. K. Rao, "Hash based approach for providing privacy and integrity in cloud data storage using digital signatures," International Journal of Computer Science and Information Technolo- gies, vol. 5, no. 6, pp. 8074–8078, 2014.

[67] D. Hofheinz and T. Jager, "Tightly secure signatures and public-key encryption," Designs, Codes and Cryptography, vol. 80, no. 1, pp. 29– 61, 2016.