International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 2, Issue 2, April-June, 2024
Available online at: https://itjournal.org/index.php

# The Creation of a Method to Handle the Cyane Issues Facing Indian Smartphone Users

**G Prasad Babu[1], Dr Ashish Chandra Swami[2], Dr Sikhakolli Gopi Krishna[3]**

[1]Research Scholar, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[2]Associate Professor, Supervisor, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[3]Professor, Co-Supervisor & Professor Sri Mittapalli College of Engineering, Guntur, Andhra Pradesh.

## ABSTRACT

**Criminals have the potential to do a broad variety of harm to people, companies, and society as a whole by exploiting vulnerabilities in the security built into the internet and the programs that run on it. Several types of attacks, including Denial of Service (DoS), Distributed Denial of Service (DDoS), Probe, Remote to Local (R2L), User to Root (U2R), HeartBleed, Exploits, Malware, Botnet, and Worms, have made a great number of online services and applications very susceptible to attack. A significant problem with the Internet is that it allows bad actors to hide their tracks by faking the IP address of the file that originated from which they obtained the file. Internet protocol (IP), which is responsible for operating the Internet, is the reason why this is possible. IP is responsible for making it possible. This vulnerability has been exploited by hackers in a number of attacks, causing widespread disruption to a wide variety of online services and activities while also causing irreparable harm to the individuals who were the targets of these attacks. Researchers have been looking for a solution to the problem of how to stop attacks on the internet like this one from happening ever since the beginning of time.**

**There have been a lot of individuals who have considered approaches to either lessen the frequency of attacks or put a stop to the growing number of assaults. Routers, security software, encryption, decoding, IP traceback, and the capacity to identify and prevent breaches are all included in this category of security tools. IP Traceback and Intrusion Detection are two technologies that have been researched in the past, and the objective of this thesis is to integrate them in order to find and avoid threats in software-defined networking (SDN). It is normal practice to utilize an intrusion detection system (IDS) to monitor the network for any odd activity or policy violations. This allows for the prompt resolution of any problems that may arise in the future. This method may be used to tackle any problems that may come up in the future. If you are aware of the origin of malicious attack packets, you may use a method known as IP traceback to locate them and then eliminate them.**

**The IP traceback system that is referred to as "SDN and MPLS Integrated Traceback Mechanism (SMITE)" will be implemented in one autonomous system (AS) that is based on software-defined networking (SDN). At this point, it is my opportunity to provide the first piece. In order to keep track of the original source IP addresses of data bits as they transit from their origin to their destination inside an AS, the SMITE protocol makes use of MPLS labels with the intention of maintaining this information. Using the strength of MPLS and the flexibility of SDN, we are able to combine their benefits in order to achieve a low false positive rate, post-hoc packet tracking, and the capacity to identify and delete a single fraudulent attack packet with little expenditures on both data and hardware. I-SMITE is the second choice available to anybody looking for an alternative to Inter-AS SMITE.**

**One of the ways that OpenFlow does this is by using software-defined networking (SDN), border gateway protocol (BGP), and multiprotocol labeling (MPLS), which is also frequently referred to as "protocol labels." IP traceback may be able to function across ASes due to the fact that information about traceback is often sent between ASes by means of BGP Update Messages. Because of this, IP traceback may be able to work despite the presence of many ASes. One of the reasons why ISMITE is so enticing is because of BGP. In this instance, we have yet another indication of the many benefits that SMITE provides you with. The third point is that there is continuing research on Intrusion Detection Systems (IDS) that make use of Support Vector Machines (SVM) to detect intrusions and selectively record IP addresses for the purpose of IP traceback. This most recent intrusion detection system (IDS) makes use of both a fraction of the NSL-KDD dataset and the whole dataset in its operational procedures. The probability of uncovering an attack is significantly increased as a result of this consideration.**

**Through the usage of the PACKET_IN event, it is possible to identify data that does not belong as well as people who have acquired access to the community network. On a daily basis, the use of OpenFlow switches for the purpose of gathering flow data has become the regular practice. You have the ability to choose which anomalous packets or flows to capture via the use of a PACKET_IN event. In the event that your network is victimized by an attack, this gives you the ability to conduct an IP traceback. The logging of events while the central processing unit is operating is one potential approach. This would result in a large reduction in the amount of RAM that is used overall. In addition, the system manages reporting operations by using inmemory structures at the manager. This results in a significantly decreased amount of memory being used in comparison to a conventional database that is based on files.**

## INTRODUCTION

Nearly everyone is now more capable than ever before of connecting to the internet, using a computer, or using an Internet of Things device. In our everyday lives, each and every one of us makes use of these technologies, and they have a big influence on our conduct, both at home and at our place of employment. Moreover, the business sector is also seeing an increase in its appeal. These days, a significant number of transactions are recorded on the internet. A variety of people from different parts of society are involved in these arrangements. These people come from the government, healthcare, social services, banking, manufacturing, and business sectors. It was formerly impossible to preserve private data digitally; now, because to recent technological advancements such as cloud storage, this is now feasible. An important step forward has been taken here. In this area, you will find records of service, medical information, and bank account information, among other things. A growing number of infrastructure operations, such as the production of power and the collection of waste, are increasingly adopting software- driven systems as their primary operational mechanism. As the number of people who depend on the Internet continues to rise and technological advancements continue to be made, hackers are becoming more and more interested in doing it.

It was discovered that one-third of the companies that were surveyed for the "Global Economic Crime Survey 2016" had been the victims of hacking. Given the frequency with which these breaches occur, they have become a matter of intense interest in the field of international finance at the present time. According to the findings of the study, various negative repercussions are caused by hacking; nevertheless, the most significant damage is done to an individual's reputation. businesses who answered reported losses of five million rupees (PS3.5 million), and about a third of those businesses reported losses of over one hundred million rupees (PS69 million). This indicates that at least half of the enterprises that responded reported losses. The findings of the "Cyber Security Breaches Survey 2020" conducted by the government of the United Kingdom reveal that hacking has developed and attained a greater level of popularity in recent years. According to the survey, during the course of the previous year, 46 percent of businesses and 26 percent of charity organizations had a data breach or hacking event. In the year 2020, Kaspersky Lab uncovered an extra 360,000 harmful files on a daily basis, as reported by the organisation. In comparison to the previous year, there has been an increase of almost 18,000 people over this time period. There is also a rise of 5.2% in addition to that.

To determine the identity of the malicious application, object- finding sensors were used in the laboratory. new harmful file types are being found on a regular basis, which means that criminals are generating and spreading new malware on a daily basis. Even though there have been considerable breakthroughs in technology, perpetrators of illegal activity may still utilize the Internet to attack people, organizations, and even the government and the military. There have been a number of internet services that have been badly affected by threats of denial of service (DoS). These are some of the most common dangers that businesses need to be aware of and try to eliminate to the greatest extent possible. Hacking and data breaches are always developing, and the techniques that are used to commit them are becoming more accessible. You probably think of a broad range of dangerous programs when you hear the term "malware." These programs are intended to steal data or cause damage to systems and networks. Malware is an umbrella term that comprises a broad range of harmful software, such as spyware, ransomware, viruses, Trojan horses, and worms. This package contains rubbish, malware, and adware all in one convenient bundle. When an individual opens an email or clicks on a link included inside an email, the email is sent to the specified computer. Through a behavior that is similar to that of ransomware, malicious software has the capability of restricting access to vital areas of a network. Not only may viruses infect animals, but they can also infect other animals. In addition, it has the capability of stealing sensitive information from the computer of the victim, as well as having the ability to destroy or damage electronic devices, rendering them useless.

Hackers sometimes utilize fraudulent emails that seem to come from legitimate businesses in order to carry out their hacking activities. This practice is referred to as "phishing." It is possible that the malicious link included in the email may convince users to click on it, placing their systems in jeopardy and perhaps revealing important information such as passwords and credit card details. With the goal of gaining access to sensitive financial information, a more sophisticated kind of email fraud known as "spear phishing" targets particular persons, companies, or groups in an attempt to get the information. The method of spear phishing is used by con artists. The individuals who make use of the systems, such as the executives and managers of corporations, are the targets of an attack. In the context of a situation, the phrase "man-in-the-middle attack" refers to a scenario in which one party covertly listens to the conversation of another party. A phrase that is sometimes used to describe this is the "eavesdropping danger." When an enemy has access to this information, they have the ability to get access to the accounts of both of the individuals who participated in the chat. In attacks that are referred to as "Denial of Service" (DoS), the target systems, networks, or websites are inundated with an excessive volume of data, which renders it difficult for them to respond to valid requests. It is possible that the criminal will even take advantage of the opportunities that are presented to them. Instances of distributed denial of service attacks, often known as DDoS attacks, are among the most advanced forms of this kind of attack. In order to get into the system they are targeting, they depend largely on personal computers and other devices that are simple to hack. Steps involved in loading SQL are as follows: Hackers are able to get access to databases using a vulnerability known as SQL injection.

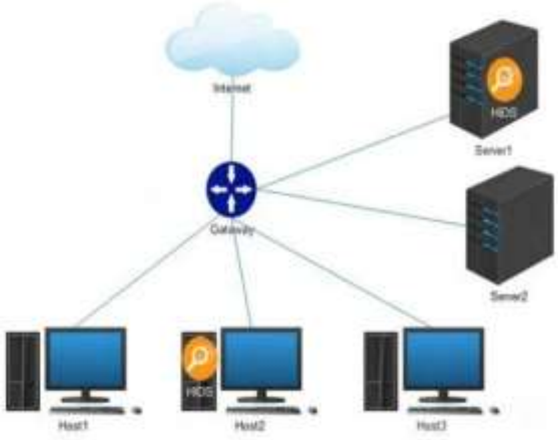

**Figure 1.3: Host based IDS**

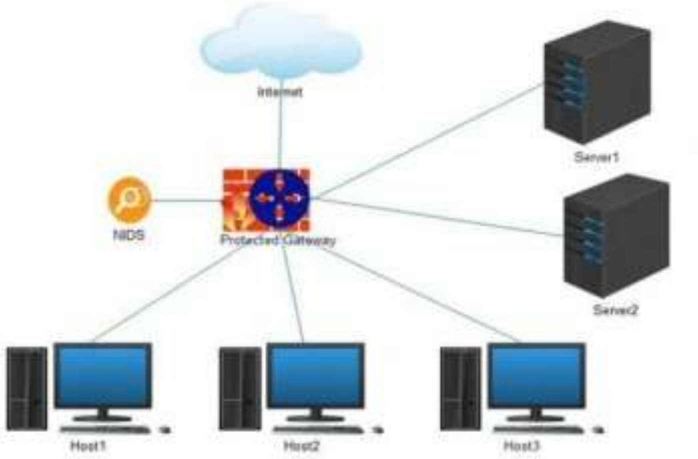

**Figure 1.4: Network based IDS**

These devices in the subsequent stages. Another word for computers that have been infiltrated is "zombies." Figure 1.1 illustrates a typical distributed denial of service attack that may be seen in its entirety. A hacked manager might unleash a data deluge on weak intermediate sites, which are commonly referred to as "zombies." This kind of assault is typically carried out by these sites. A hacker may flood devices with data in order to make them unworkable. One example of this would be the Web Server for example.

## LITERATURE REVIEW

Research uses several established behavioral models to explain why users adopt or ignore cybersecurity practices. Prominent among them are the Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and the Technology Acceptance Model (TAM). These models help researchers understand user attitudes, motivations, and decision-making processes in digital environments**.**

1. PMT suggests that individuals act based on how severe they think a threat is and how confident they are in their ability to protect themselves. Literature shows that if users do not believe cyberattacks pose serious harm—or feel unable to follow security protocols—they are unlikely to adopt safe practices.
2. PMT suggests that individuals act based on how severe they think a threat is and how confident they are in their ability to protect themselves. Literature shows that if users do not believe cyberattacks pose serious harm—or feel unable to follow security protocols—they are unlikely to adopt safe practices.

## BACKGROUND RESEARCH

Due to the fact that cybersecurity is one of the most major threats that businesses face, companies are starting to think about taking steps to protect themselves. Countries all around the globe, including the United States of America, the United Kingdom, and India, have enacted anti-hacking laws in order to protect their people' data and ensure their safety. As the problem of hacking continues to grow, regulations have been implemented for the internet in response to the current situation. The Internet of Things (IoT), smart grids, and other cyber- physical technologies are just a few examples of the many different areas of technology that are seeing an increase in cybersecurity needs. Let's forget about the notion that cybersecurity is only a subject of computer science or engineering; rather, it calls for a more comprehensive perspective. Without a shadow of a doubt, end users and technology protection measures are interdependent from one another.

People and technology alike need a strong foundation in order to be successful in the face of cybersecurity threats. Contributions to what are known as sociotechnical views come from a wide variety of individuals, including end users, legislators, and those responsible for developing security regulations. These individuals share their thoughts and actions. Hackers are capable of performing a wide range of functions, including those of attackers, guards, and computer users. Keeping this assumption in mind, the consequences for noncompliance have been created with the intention of ensuring compliance with the Information Security Policy as well as other administrative security rules. At the time that these standards were being created, however, security professionals neglected to take into consideration how important it was to provide security personnel with a working atmosphere that was both friendly and practical.

A cryptographer by the name of Auguste Kerckhoffs lived throughout the centuries of the 1800s. It was his article in 1883 titled "Kerckhoffs' principles," which outlined six rules for the development of military ciphers, that brought him to the forefront of the field (Kahn). The actions of humans served as the foundation for three of the six notions that were examined. A landmark work that Jerome Saltzer and Michael Schroeder released over a century later outlined eleven design principles to assure the security of computer data (Saltzer and Schroeder). This study was important since it was the first of its kind. Three out of the ten rules dealt with issues that are relevant to persons and have an effect on them. The people understood the value of individuals in ensuring the safety of the community for themselves. There have been several studies conducted within the industry that indicate that human error is the primary cause of security breaches (Symantec, Verizon, 2020; IBM, 2020). As per the findings of several research, the weakest link in any security system is the human element. A human being was engaged in 85 percent of all leaks (DBIR), according to an estimate provided by Verizon for the year 2021. Errors, the loss of assets, theft via social engineering, and seven other types of events are one of the things that are mentioned in the study.

## PROCEDURES AND SCHEMAS

The use of MPLS in SDN allows SMITE to avoid the limits of traditional traceback systems. This allows the company to lower the amount of money spent on hardware and the amount of data storage that is required, all while maintaining a low false positive rate. You are able to do more with SMITE than just begin a traceback after the fact; you are even able to trace back a single false attack packet. When an entry OpenFlow switch starts a PACKET_IN event on a software-defined network, the main job of SMITE is to obtain and record the source IP address of incoming packets. This is accomplished by retrieving and logging the source IP address. In order to ensure that a packet has the right source IP address, it is tagged with an MPLS label, which is also referred to as the SMITE Label, at the entry switch. After this, the packet is modified with the new name, and it is then sent to the subsequent node in the network. Instead of the normal multiple OpenFlow fields, the flow table entries of the OpenFlow switch use short MPLS labels. multiple OpenFlow fields are often used. This saves space in both the processing and storage portions of the system. The size of the flow table, the matching costs while data plane packets are in transit, and the need for packet-log storage for traceback are all greatly reduced as a result of this adjustment.

Because of the amount of time and effort that is necessary, the expansion of the network is hampered. Given the dynamic nature of MPLS label creation and encoding on moving packets, the adaptability of software-defined networking (SDN) has the potential to significantly enhance the functioning of SMITE. Furthermore, in addition to researching MPLS, we also studied the idea of delivering the traceback data using a Virtual Local Area Network (VLAN). However, there are a great deal more advantages to using MPLS as opposed to VLAN. There are around four thousand different virtual local area networks (VLANs) that may be individually recognized by the 12-bit VLAN ID. This ID can take on values ranging from zero to forty-ninety-five (with a few being designated for particular uses).

There is a VLAN tag field in the Ethernet header that is two bytes long, and that is where the VLAN ID is stored. Ethernet switches have the ability to manage traffic from distinct VLANs in a variety of different ways, depending on the identification of the VLAN. These methods include accepting, blocking, or promoting certain patterns of VLAN traffic. It is unfortunate that the VLAN tag is not sufficient to convey the source IP address. If you want to utilize additional data in the IP header, you will need to do so. Because of this, it is evident that the use of a separate object for IP traceback is rendered worthless, with the exception of the data included in the IP header. In addition to this, MPLS may support a considerable number of standards, while VLAN may only support Ethernet. When using MPLS, rather of using large network names, short route labels are used. The packet routing approach is now easier to comprehend, which has resulted in the network being managed in a manner that is both much more efficient and less complicated. As a result of the rigorous Class of Service (CoS) and Quality of Service (QoS) guarantee, the network is able to effectively manage and organize data in order to fulfill all of its requirements.

See Figure 3.1 for an illustration of the construction of the SMITE device. (i) linking Macs to ports and ports to IPs; (ii) maintaining SMITE Flow; (iii) encoding and decoding MPLS labels; and (iv) the REST API module are the four key components included inside this system. Port-to-MAC address mappings are stored in the MAC address database, whereas IP address mappings from ports are stored in the area reserved for the ARP table. The following two essential data structures are looked after by this utility: both Mac-to-Port and Port-to-IP ports. The Media Access Control (MAC) address table is the very first item that is generated once a network is booted up. When there is a change in the status of a port or switch, it is often updated. An ARP table is filled with information whenever the first packet in a flow arrives, which is referred to as the PACKET_IN event. When flow items in the switch come to an end, the data structures for the ARP table are likewise filled in. When a manager adds a flow entry for the next packet in the same flow at the switch, a new PACKET_IN event is generated when the packet enters the network. This occurs just as the packet is entering the network.

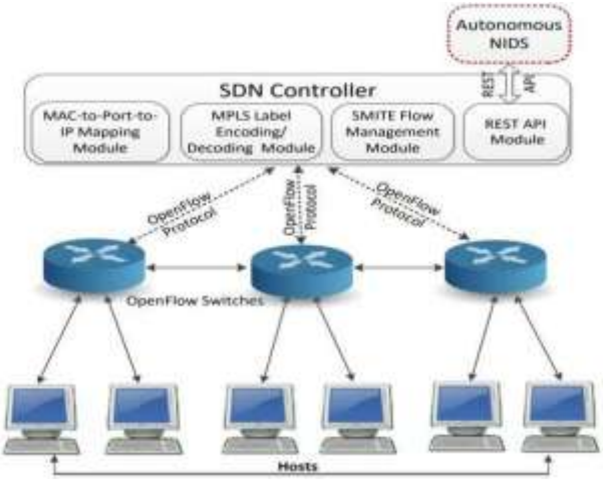

**Figure 3.1: SMITE Architecture**

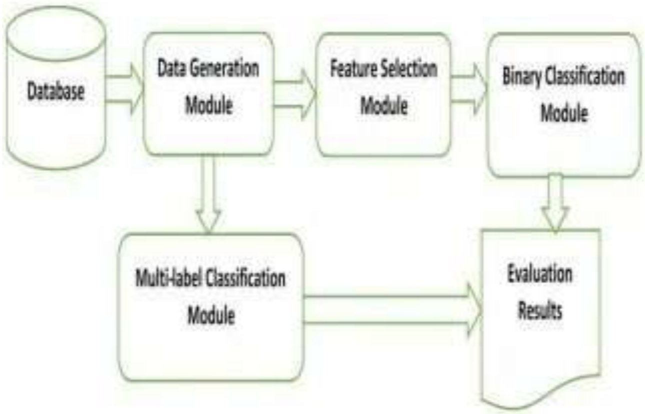

**Figure 3.6: Proposed framework**

The module for the production of data is an essential component of the data analysis process. This aspect is broken down into its component parts and shown in Figure 3.6. A timestamp that is one second in the past is obtained by the parser software once the extraction process has been completed. Additionally, the raw network data are obtained. Within a fraction of a second, the software that functions as a packetizer is able to extract the essential features of each individual packet. The date, the protocol, the MAC IDs of the sender and receiver, the ports of the sender and receiver, flags (including SYN, ACK, PSH, RST, FIN, ECE, CWR, and URG), and the size of the packet are all pieces of information that are contained in each and every packet. In order to determine the identity of a packet, certain distinctive qualities are necessary.

The sessionizer module is responsible for receiving data that is generated at the packet level for each flow that is directed to the destination. This data is then used to read and generate session-level data. As a result of the fact that the identification is carried out at the conclusion of the destination sequence, the sessionizer includes information that is specific to the target. A key is generated by the labeling module by using the data obtained from the CIC DoS datasets. The labeling module uses the five tuples {SourceIP Address, DestinationIP Address, P rotocol, SourceP ort, Destination P ort > to execute the key generation process. Through the use of this key, the packet flow may be recognized and designated on the dataset. Consequently, each and every feature set The components that show the accuracy and area under the curve (AUC) are the components that make up each feature in the set that was subjected to logistic regression analysis.

## TESTS AND FINDINGS

Some examples of research techniques that do not include trials include surveys, correlational schemes, and studies that compare the similarities and differences across causes. Researchers that use a causal-comparative methodology begin by comparing the two groups after first discovering the factors that differentiated them from one another. Correlational statistics are used by researchers in correlational design in order to seek for correlations between the variables being studied. Through the use of survey research, it is possible to get insight into the behaviors, attitudes, and feelings of a group. Among the techniques that might be effective for data collecting are surveys and prepared conversations.

A qualitative technique is used in order to investigate and ascertain the relevance of a human problem from the perspectives of a variety of persons or groups. By using it, you will be able to decide the most effective use of technology in any particular circumstance (Blandford). Not only does this method provide freshly collected data, but it also gives specifics on the viewpoints, ideas, and motives of customers. This method is often used for the purpose of gathering information in natural areas. It is the researcher's ability to deduce the overarching themes from the specifics that determines the usefulness of the data. By using this method, the constructivist and transformational pedagogy of research is effectively used. Case studies and grounded theories are two examples of qualitative research approaches that might be used. Using this strategy, researchers have the potential to get a more comprehensive knowledge of the topic of their study by merging qualitative and quantitative data. The fundamental idea behind this tactic is that if you mix qualitative and quantitative research approaches, you will be able to get a more comprehensive and precise understanding of the challenge you are attempting to investigate. The functional approach tends to be the guiding principle for studies of this kind. It is possible to get a broad range of styles at a number of different shops. In the realm of mixed-methods techniques, there are three basic types

## CONCLUSION

There are a multitude of security measures that have been offered in order to stop and limit the many types of hacking. Some of these ways include IP traceback, intrusion detection, intrusion prevention, encryption and decoding, firewalls, antivirus software, and many more. Our objective in this study is to improve the safety of the network by integrating the detection of intrusions with the tracking of IP addresses. The process of finding invasions has been approached from a wide variety of perspectives up to this point. On the other hand, these intrusion monitoring systems are plagued with a multitude of issues. Any method of attack detection is subject to the two primary problems of false positives and false negatives. False positives refer to packets that are improperly detected as attacks, while false negatives refer to packets that are incorrectly classified as normal. In the event that detecting and preventing attacks is not sufficient, we need to acquire a method that can reliably identify the origin of assaults in order to ensure that those responsible are held accountable. IP traceback is a practical response to the problem of cyberattacks, which shows the real source of a phishing message. This strategy is one of the practical approaches.

If you use IP traceback, you will not be able to stop or avoid an attack. Instead, its objective is to determine the origin of the problematic packet, either during or after an attack. This may be done either during or after the attack. The identification of the offender, the disclosure of their name, and the implementation of measures to guarantee that they are held accountable for the attack are the key goals of IP traceback. The combination of an intrusion detection system (IDS) with a traceback mechanism is a logical step that would considerably enhance the level of security that existing networks possess. The public has been made aware of certain logging IP traceback systems in order to counteract the many different types of hacking. The SPIE, which was developed by Snoeren and colleagues, is an instrument that has received a lot of attention in this area. Certain servers along the path of the network are responsible for storing information on packets that are currently in transit. According to the authors of the proposal, in order to generate a packet fingerprint, one should make advantage of the fixed aspects of the IP packet header. They recommend avoiding the ToS, TTL, Checksum, and Options fields, which are subject to major changes.

## REFERENCES

[1]. PricewaterhouseCoopers, PwC, Global economic crime survey 2016, 2016. [Online]. Available: https://www.pwc.com/gx/en/economic- crime- survey/pdf/ GlobalEconomicCrimeSurvey2016.pdf (visited on 11/03/2020) (page 1).

[2]. Department for Digital, Culture, Media and Sport, Govt. of UK, Cyber security breaches survey 2020, 2020. [Online]. Available: https://www.gov.uk/government/ statistics/cyber- security-breaches-survey-2020/cyber-securitybreaches-survey- 2020 (visited on 11/03/2020) (page 1).

[3]. Kaspersky Team, Kaspersky malware detection 2020, 2020. [Online]. Available:https://www.kaspersky.com/about/press- releases/2020_the-numberof-new-malicious-files-detected-every-day-increases-by-52-to360000-in-2020 (visited on 11/03/2020) (page 2).

[4]. P. G. Neumann, “Inside risks: Denial-of-service attacks,” Commun. ACM, vol. 43, no. 4, p. 136, Apr. 2000, issn: 0001- 0782. doi: 10.1145/332051.332797. [Online].Available: https://doi.org/10.1145/332051.332797 (pages 2, 3).

[5]. G. Carl, G. Kesidis, R. R. Brooks, and Suresh Rai, “Denial- of-service attack-detection techniques,” IEEE Internet Computing, vol. 10, no. 1, pp. 82–89, 2006. doi: 10. 1109/MIC.2006.5 (pages 2, 14).

[6]. Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics,”

[7]. IEEE Transactions on Information Forensics and Security, vol.

[8]. 6, no. 2, pp. 426–437, 2011. doi: 10.1109/TIFS.2011.2107320.[Online]. Available: https://doi.org/10.1109/TIFS.2011.2107320 (pages 2, 14, 78).

[9]. V. M. Igure and R. D. Williams, “Taxonomies of attacks

[10]. and vulnerabilities in computer systems,” IEEE Communications Surveys Tutorials, vol. 10, no. 1, pp. 6– 19, 2008. doi: 10.1109/COMST.2008.4483667 (page 3).

[11]. N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, “Network attacks: Taxonomy, tools and systems,” Journal of Network and Computer Applications, vol. 40, pp. 307–324, 2014, issn: 1084-8045. doi: https://doi.org/10.1016/j.

[12]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow:

[13]. Enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008 (pages 6, 11, 27, 44, 59).

[14]. H. Kim and N. Feamster, “Improving network management with software defined networking,” IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, 2013 (pages 6, 11, 27, 44, 59).

[15]. T. D. Nadeau and K. Gray, SDN: Software Defined Networks: an authoritative review of network programmability technologies. " O’Reilly Media, Inc.", 2013 (pages 6, 11, 27, 44, 59, 78, 79).

[16]. S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, “Are we ready for SDN? implementation challenges for software- defined networks,” IEEE Communications Magazine, vol. 51, no. 7,pp. 36–43, 2013. doi: 10.1109/MCOM.2013.6553676

[17]. (page 6).