Analyzing the Behaviour of DDoS Cyber Attack

Tanvir Fatima Nail Bukht
fatimaishtiaq7@gmail.com
Institute of Southern Punjab Multan, Pakistan

Abstract
The digital environment of cyber society is also being affected by intruders, cybercriminals and neighbor countries. Because of this, ongoing research in the field of cybersecurity is playing an important role and a huge impact on society. The main objective of this research is to measure the level of cyber-attack and analyze the behavior of cyber-attacks via ICT (Information and communications technology) tools. Two organizations of Pakistan have been chosen to analyze their behavior. We conducted the result of DDoS attack by using Wireshark and LOIC. DDoS attack is chosen to analyze the behavior (before attack, during and after attack) of systems or services. This cyber-attack is targeted at State Bank of Pakistan, Passport & Immigration. We can improve security by knowing gaps weak points and solutions to control crimes. This research will also help other most sensitive organizations of Pakistan such as the Federal Public Service Commission, Ministry of Finance, Revenue and Economic Affairs, Ministry of Interior,

Keywords:
Cybersecurity, cybercriminals, network activity, behavior of cyber-attacks, DDoS attack.

1. Introduction

The cyberattacks were even more complex and better. In General, an economic system, and organizations in our society rely heavily on information networks and IT solutions. These value systems are therefore a major concern. The Cybercrime report and the safety investigation to confirm that the injection of malware, phishing, cyber-theft, and bot attacks are common approaches for cyber-attacks to obtain sensitive Material and so that the organizations harm [1]. The growing number of cyber attacks on digital technology and communications networks has drawn the attention of ICT professionals (information and communication technologies), Cybersecurity wings and other security officials to improving security. Securing the information, network, records, and the application has come to be one of the biggest challenges of the present. Cyber security is an incredibly important part of the IT world as it improves progress in protecting data, applications, systems and information against illegal access or attack, as well as defending information, software, networks and against unauthorized access or attacks [2].

Cybersecurity plays an essential role in the field of ICT. Hence, Protecting the network, data information, and application have become a major challenge in providing user-friendly security services [3]. Cybersecurity is important for both the wireless and wired parts of the system [4]. The most important task of a cyber-security analyst is to protect a network of damage. Many technical advances in information security and networking have allowed analysts to more closely monitor and detect threats[5]. From the studies[6], [7], it is identified that the 21st century becomes more vulnerable and insecure. Hence, it becomes important to understand the cyber-attacks either targeted before, after and during their occurrence to provide better security for critical systems. Without understanding the vulnerability of the network becomes very complex to predict a possible attack. So, it is important to analyze the network to provide an intuitive idea for protecting the network[8].

2. Literature Review

The security of digital technology is also the primary duty of the organizations, professionals, developers, and government to offer their customers a secure service. The internet has become an important part of everyone's life. It is widely used in homes, offices, schools, hospitals, and businesses. It is a tool that lets you keep track of things, stay up-to-date with news, and communicate with everyone. The progress of life has also changed but poses a threat to privacy, identity, personal resources, data, and valuable information. In the warfare against cyber-attacks, cybersecurity is a delicate problem in the world of security companies and governments experiencing every effort to deploy or implement various tools and techniques to protect their data and private information in order to keep their business running [8], [9].

A distributed-denial-of-service attack is also known as a DDoS attack. In this type of attack, the attacker sends a large number of packets from a large number of host computers to the computer of the victim to terminate normal services, which exhaust victims' IT resources like memory and processor, and Ultimately, this leads to a lack of data available for authorized users. The attacks of the denial of Service and the denial of distributed service have repeatedly raised serious problems in the research community. In 1999, the first distributed denial of service attack was reported by

Manuscript received March 5, 2025
Manuscript revised March 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.3.22

Computer Incident Advisory Capability (CIAC), and most of the DoS attacks that took place were distributed[10].

The security of the network domain is also required as the usage of the networks increases day by day. Other data and information are generated. Real-time defense of information and data is becoming increasingly difficult for today's businesses. DDoS (Distributed Denial of Service) attacks are commonplace today [11], [12]. Trojans of the Denial of Service (DoS) prevent the functioning of a function or source [13]. If enterprise security requirements are not very high, we can take the protection of by-hop encryption. Or, if the demands on commercial requirements are high, we can use end-to-end cryptography [14][15].In a DDoS attack, the attacker has a great influence on the victim by multiplying the attack power of many cyber agents. It is possible for an attacker to check many computers on the Internet before an attack is launched. In fact, these agents in the public network, and the attacker can abuse their vulnerabilities by introducing malicious Codes or other piracy techniques to control them [7][10]. Denial of Service attacks can disrupt the following, communication and protection systems. Floods are a kind of DoS attack in which the attacker sends many messages to a tar network. Another important analysis concerns the size of the message that should be done for both situations[11][16][17]. Today's network infrastructure is threatened by DDoS attacks. There are many methods for defense against DDoS attacks but these techniques need to improve for more efficiency due to the advancement of attackers and their attacking tools and methods. It is a big task to mitigate DDoS attacks, but it is necessary to prevent these attacks. But more efforts are required to develop the organization's network security.

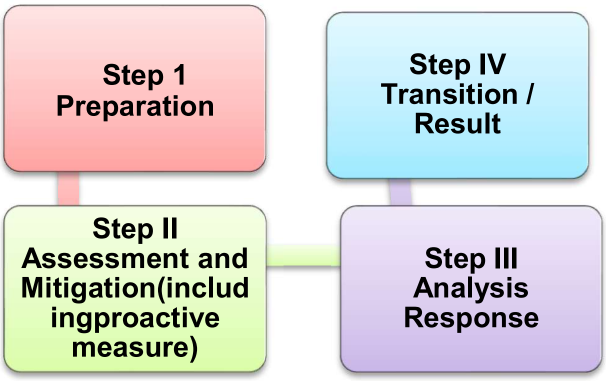


Figure 1 proposed model for analyses the behavior of cyber attack

Mitigation of the DDoS attacks can be divided into three classes, i.e., before the attack, during attack, and after the attack[18].

3. PROPOSED MODEL

This comprises of the proposed security model, which is essential to find and analyze the cyber-attack. The proposed model consists of four steps. Each step has its importance, the initial or first step is necessary for making preparation for the analysis of attacks. The second step assesses and identifies the modification practices for attacks. Dependent on the analysis of the response gained from the system is discussed in step three. The fourth and last step gives transition or results.

3.1 Preparation: Step One

Cybersecurity is perhaps the best challenge of present-day times. Preparation is necessary for analyzing the behavior of cyber attacks. We create an environment for our simulation/analysis by using whir-shark and LOIC. Wireshark is a very useful tool for analyzing, it helps us for detecting behavior. We select 2 top organizations for our measurements. As an ever-increasing number of users of the Internet and cell phones, controllers need to guarantee that data correspondence advances (ICTs) are shielded from attackers. Well, almost everything hangs on ICT, which makes companies more vulnerable. Several international organizations have committed to controlling cyber threats. Most of these organizations support global support in addressing cybercrime problems. Therefore, a secure Internet available always is important. Hackers have reached a level that cannot be solved with conventional self-protective countermeasures. The cyber securities are as an immediate measure against explicit attack to respond on networks and computers.

We create an environment for analyzing DDoS attacks. DoS attacks (denial of service) are widespread in today's Internet world. With increasing attacks, internet servers and network devices are more vulnerable than ever. For a similar explanation, associations and individuals who have large servers and data on the Internet are planning and investing heavily to protect themselves against a range of cyber-attacks, including denial-of-service. In a DDoS attack, the attacker has a great influence on the victim by multiplying the attack power of many cyber agents. It is possible for an attacker to check many computers on the Internet before an attack is launched. In fact, these agents in the public network, and the attacker can abuse their vulnerabilities by introducing malicious Codes or other piracy techniques to control them. These damaged machines can consist of hundreds or Thousands of Numbers. These compromised machines can consist of hundreds or thousands of numbers. They act as agents of the attacker and are commonly referred to as "zombies". The whole collection of zombies is frequently referred to as "botnets". The size of the botnet decides the size of the attack. The researchers point out that the means to combat these attacks require further research [7]. Through Preparation step we able to understand that protection against cyber attacks needs to be improved.

3.2 Assessment and modification: Step Two

The attackers now have to attack quickly with the current attack tool in order to obtain financial benefits and other benefits by rejecting the victims ' resources for the real users or shamefully rejecting them. We deduct data by using Wireshark, LOIC and start its assessment or modification. The ability of a deduction DDoS and the noise reduction techniques are based on its accuracy and reliability, so that false-positive and false-negative results can be reduced in a System. Packages must not overcome the mitigation mechanism. The associated file attacks the traffic (false negative) and reaches the victim. Packets belonging to real traffic (false positive) must not be discarded. Countermeasures against DDoS are generally divided into three types of techniques, which are listed below.

- Reactive techniques
- Pro-active techniques
- Survival techniques

In reactive techniques, the victim is challenged with a DDoS attack on his services. Therefore, a detection and defense method is called to trace the origin of the attack and filter traffic out of the identified sources.

In proactive techniques, the objective is to recognize an attack before it can arrive at the destination. After discovery, a mitigation methodology can be called quickly to channel or restrict attack traffic.

In survival techniques, equipment and systems that can become victims of DDoS attacks, they have sufficient resources to provide services to authorized users in the event of a DDoS attack. Resources such as CPU power, bandwidth, memory, etc. will be sufficient and resource redundancy will be maintained if needed [7].

But in our research, we use the proactive technique because it's more effective for our research than other techniques. We can discover attacks traffic or can mitigation easily. We know that detection is of threats and attacks on networks for years, one of the biggest challenges for cybersecurity. Network Intrusion Detection Systems (NIDS) used to detect unauthorized access by analyzing the network. New and more advanced types of attacks require new and more sophisticated defenses. For example, a new threat class called Advanced Persistent Threat (APT) is a well-trained adversary and resource with sufficient resources. The early detection of cyber threats in the observation sequence test is performed by examining the correlation between each trigger identified in the sequence by identifying possible types of attacks. To be specific, as they go through the test sequence. We can find all valid different trigger levels for each window of constituent network activity. It should be noted that each activity window in the sequence of monitoring may correspond to multiple activators forming different levels[19].

3.3 Analysis response: Step Three

Cyber-attackers can be illogical or selective and attack both large and small public and private sector enterprises. The first step for companies looking to improve their computer security skills is to develop a better understanding of the nature of the threat to them. It will not be possible to improve the ability to restore information security in the organization without first identifying the potential causes of harm and their potential impact.

Denial of Service attacks can disrupt the following communication and protection systems. Floods are a kind of DoS attack in which the attacker sends many messages to a tar network. Another important analysis concerns the size of the message that should be done for both situations [16]. There are two ways to apply behavioral detection methods: abuse detection and anomaly detection. Detecting abuse looks for specific behaviors that are considered harmful [20], [21]. While the anomaly-based approach satisfies unusual and unexpected behavior [22], [23]. The detection of misuse is more reliable in terms of recognition performance, has less false positives and often no false-negative results, but has two main disadvantages. First, the classification of a series of harmful schemas (signatures) takes a long time and the activity is an activity error when performed by human experts. It requires regular updates, just like modern antivirus systems do today. Second, it is unable to detect harmful code that has no known harmful behavior patterns, and therefore its ability to recognize new behaviors is very limited. On the other hand, detection of anomalies can detect any malicious behavior in the system that becomes a learned profile. Therefore, it can intelligently detect unknown and hidden security threats. In fast-changing environments, detection of anomalies has a high rate of false alarms compared to malicious methods.

3.4 Transition or Results: Step Four

The transitional step is a critical and vulnerable time. We attach great importance to the planning and implementation of the transition, which requires comprehensive cooperation with customer management. For analyzing the behavior of cyber attack we use two organizations of Pakistan such as State Bank of Pakistan, Passport & Immigration. We conduct results before the attack, after the attack, and during attack. At the start point of analyzing the attack in this step, we will analyze before the behavior of DDoS attack that will help us to know the difference between before and during the attack and about its traffic. Afterward analyzing before and during attack then we will analyze after attack behavior that we help us to know its effect and performance. Through the help of results, we can easily measure the behavior of attack, delay time, packet capturing, response, average bytes, bits, etc and conduct results that which one organization's security system is best.

4. Behaviors of cyber attack

4.1 Before Attack

When a user is not receiving an expected level of service from an IT service. The expected service levels are based on SLAs or service level agreements. Well, an accident can generally be something that does not work properly. According to SANS, incident response plans must include preparation, identification, containment, eradication, restoration, and lessons learned. Preparation like what we need to know.

The identification shows what happens to the system. Containment ensures that things are controlled. The Eradication/extermination helps us to eliminate the real virus and eliminate the things that cause the breakdown of the service. The accident response plan is really under control. If we want to develop an incident response plan and know what is going on before an attack, this is a bit more difficult as we never know when an attack will begin. We really need to identify or understand our critical system and identify support services for those systems. Power failures are another critical system that can lead to serious accidents in the event of a data center failure.

4.2 During the attack

During the attack, we have to keep in mind two main steps that are Don't panic and Execute your plan. If we are at the mercy of an attacker, don't paint. It's very hard to do but the worst thing that we can do is panic because what it's all about happens doing random things and we do not think logically about what's going on in the attack. If we are in a panic, we can lose some important steps. We may also put the incident response plan in place. The next step is the execution of the plan. The incident response plan you set should come into effect as soon as an accident is activated. Make sure you know the incident response plan and know who is doing what and when.

Communication is an important part of any attack. Therefore, when an attack occurs, you must ensure that you are communicating and remember that the tools are not as important as the process when you are communicating. The tools that you can use to manage the emergency plan or part of the incident plan may not work. Therefore, you should focus on your processes and on the entire incident response plan, not on the tools that are available to you.

Do not turn off any system during an attack. Some attacks will come from internal systems that have been compromised. Malware can also live in memory. So, if we interrupt the power supply to the system that is suffering or being attacked, the data can simply be erased. Therefore, we need to make sure that the network cable is unplugged. We must remember that in an attack, the goal is to reduce the damage. Therefore, we must first find out where the damage occurs and what causes it. Therefore, it is possible to check network protocols, server logs, access logs, network traffic, and authentication. All this becomes very important during an attack. So, we used network protocols and access logs to determine who had access to the system and what files were encrypted during the attack. So, we converted the file system to read-only mode. What he did was to prevent the attack from remaining. He avoided the offensive computer, we did not know who he was then. We used this server and just made it read-only, so no more files could be written.

We could find the criminal system because of the access logs and server access logs, and we cut the network for that and called the person saying that you have something with your computer, which I need you to unplug the network cable. And in the end, we will prepare ourselves to restore the lost information.

4.2 After attacks

No matter any attacks like malware, ransom-ware attack, and denial of services attack may affect your system or data. But after the attack first, you have to conduct a meeting that helps to understand what happened during the attack and also allows protecting your network or system better for the future.

The second most important is the documentation; Documentation must be collected. It is necessary to organize it in a timeline, to fill in the gaps left by other people, and to share the lessons learned. The lessons learned are important, especially because the management knows exactly what has happened. And best of all, it's a timeline, and it's good for documenting people within that timeline, so you know who did what, when, and how the problem was solved. The Lessons Learned document should include what happened, what happened, what was not successful, how the attack is planned in the future, or what we patch for the future, as well as all security checks

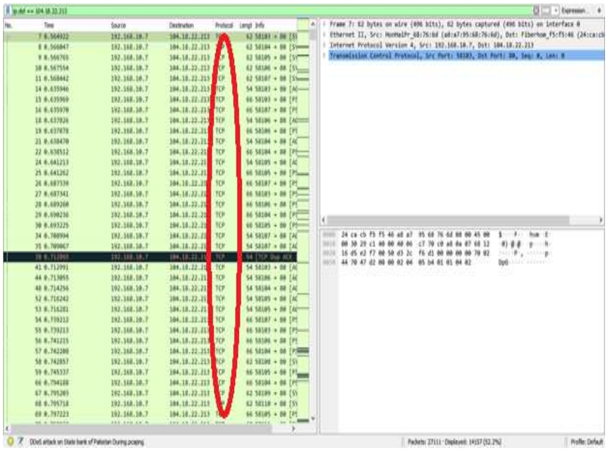
If the attack has caused damage, it must be repaired. If the attack has identified new threats, we need to face this threat. If the attack has identified new vulnerabilities, these vulnerabilities must be addressed. And when the attack has happened, we have to assess the risk. This is one of the other important points after the evaluation attack.

5. Results

One of the most sensitive organizations of Pakistan has been chosen to analyze their behavior. This cyber-attack is targeted at the State Bank of Pakistan. All the results are collected or analyzed via LOIC and Wireshark simulation tools. In addition, we have taken parameters such as (# packet loss, communication delay, traffic While analyzing the behavior of DDoS attack in Pakistan's major services/servers. Each service/server is analyzed in three ways i.e. before, during and after the target of DDoS attack.

5.1 State Bank of Pakistan

State bank of Pakistan is a leading organization in Pakistan, which runs more than 100 banks. It is a financial resource for their customers, banks and government institutes to run their organizations. Hence, State Bank of Pakistan is chosen to analyze the behavior. Figure 2 illustrates the pinging of SBP and executes its code in Wireshark tool. Initially, the IP address of SBP (104.18.22.213) is used in Wireshark tool to work in simulation environment as shown in Figure 2. Wireshark view of a pcap file storing raw telescope data belonging to Conficker worm



```
ip.dst == 104.18.22.213

No.  Time        Source         Destination     Protocol  Lengt Info
 7   0.564922    192.168.10.7   104.18.22.213   TCP       62 58103 → 80 [S
 8   0.566047    192.168.10.7   104.18.22.213   TCP       62 58104 → 80 [S
 9   0.566765    192.168.10.7   104.18.22.213   TCP       62 58105 → 80 [S
10   0.567554    192.168.10.7   104.18.22.213   TCP       62 58106 → 80 [S
11   0.568442    192.168.10.7   104.18.22.213   TCP       62 58107 → 80 [S
14   0.635946    192.168.10.7   104.18.22.213   TCP       54 58103 → 80 [AC
15   0.635969    192.168.10.7   104.18.22.213   TCP       66 58103 → 80 [P
16   0.635978    192.168.10.7   104.18.22.213   TCP       66 58107 → 80 [P
18   0.637826    192.168.10.7   104.18.22.21    TCP       54 58106 → 80 [AC
19   0.637878    192.168.10.7   104.18.22.21    TCP       66 58106 → 80 [P
21   0.638470    192.168.10.7   104.18.22.21    TCP       54 58104 → 80 [AC
22   0.638512    192.168.10.7   104.18.22.21    TCP       66 58104 → 80 [P
24   0.641213    192.168.10.7   104.18.22.21    TCP       54 58105 → 80 [AC
25   0.641262    192.168.10.7   104.18.22.21    TCP       66 58105 → 80 [P
26   0.687539    192.168.10.7   104.18.22.21    TCP       66 58107 → 80 [P
27   0.687341    192.168.10.7   104.18.22.21    TCP       66 58103 → 80 [P
28   0.689268    192.168.10.7   104.18.22.21    TCP       66 58106 → 80 [P
29   0.690236    192.168.10.7   104.18.22.21    TCP       66 58104 → 80 [P
30   0.693225    192.168.10.7   104.18.22.21    TCP       66 58105 → 80 [P
34   0.708994    192.168.10.7   104.18.22.21    TCP       54 58107 → 80 [AC
35   0.709067    192.168.10.7   104.18.22.21    TCP       54 58107 → 80 [AC
39   0.712059    192.168.10.7   104.18.22.21    TCP       54 [TCP Dup ACK
41   0.712091    192.168.10.7   104.18.22.21    TCP       54 58103 → 80 [AC
44   0.713955    192.168.10.7   104.18.22.21    TCP       54 58106 → 80 [AC
48   0.714256    192.168.10.7   104.18.22.21    TCP       54 58104 → 80 [AC
52   0.716242    192.168.10.7   104.18.22.21    TCP       54 58105 → 80 [AC
53   0.716281    192.168.10.7   104.18.22.21    TCP       54 58105 → 80 [AC
54   0.739212    192.168.10.7   104.18.22.21    TCP       66 58107 → 80 [P
55   0.739213    192.168.10.7   104.18.22.213   TCP       66 58103 → 80 [P
56   0.741215    192.168.10.7   104.18.22.213   TCP       66 58106 → 80 [P
57   0.742200    192.168.10.7   104.18.22.213   TCP       66 58104 → 80 [P
58   0.742857    192.168.10.7   104.18.22.213   TCP       62 58108 → 80 [S
59   0.745337    192.168.10.7   104.18.22.213   TCP       66 58105 → 80 [P
66   0.794188    192.168.10.7   104.18.22.213   TCP       66 58104 → 80 [P
67   0.795203    192.168.10.7   104.18.22.213   TCP       62 58109 → 80 [S
68   0.795718    192.168.10.7   104.18.22.213   TCP       62 58110 → 80 [S
69   0.797223    192.168.10.7   104.18.22.213   TCP       66 58105 → 80 [P

Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: HonHaiPr_68:76:6d (a0:a7:95:68:76:6d), Dst: Fiberhom_f5:f5:46 (24:ca:c
Internet Protocol Version 4, Src: 192.168.10.7, Dst: 104.18.22.213
Transmission Control Protocol, Src Port: 58103, Dst Port: 80, Seq: 0, Len: 0

0000  24 ca cb f5 f5 46 a0 a7  95 68 76 6d 08 00 45 00   $....F.. .hvm..E.
0010  00 30 29 c1 40 00 40 06  c7 70 c0 a8 0a 07 68 12   .0).@.@. .p....h.
0020  16 d5 e2 f7 00 50 d3 2c  f6 d1 00 00 00 00 70 02   .....P., ......p.
0030  44 70 47 d2 00 00 02 04  05 b4 01 01 04 02         DpG..... ......

DDoS attack on State bank of Pakistan During pcapng    Packets: 27111 · Displayed: 14157 (52.2%)    Profile: Default
```

Figure 2 Illustration while analyzing the State Bank of Pakistan

Figure No. 2 shows packet capturing using Wireshark and detect source address (192.168.10.7) and destination address (104.18.22.213). and it shows DDoS attack TCP flooding.

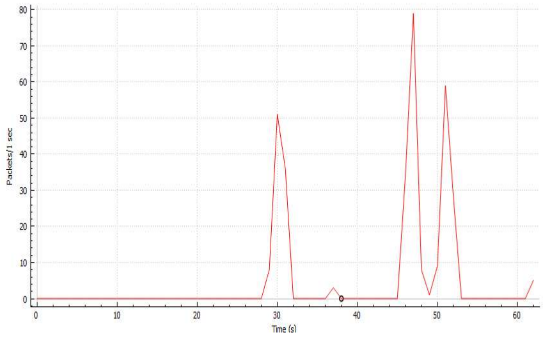


Figure 3 Illustration before the DDos attack on State Bank of Pakistan without all packets.

The graph (shown in Figure No. 3) indicates DDoS attack's results those are analyzed by using Wireshark and LOIC. The above graph consists of two components such as level of DDoS attack and time taken to reach a destination. At initial level, before the target of DDoS attack on State Bank of Pakistan, we captured 1154 no of packets which are transferred in 60 seconds of time duration to reach a destination while red line indicates the level of cyber attacks.

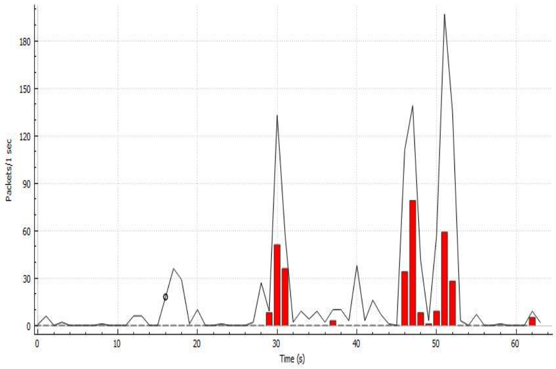


Figure 4 Illustration before the DDos attack on the State Bank of Pakistan with all packets.

The graph (shown in Figure No. 4) indicates all packets with DDoS attack's results that are analyzed by using Wireshark and LOIC. As compared to the above graph, this consists of three components such as packets, errors and time taken to reach a destination. Here the same 1154 no of packets are transferred in 60 seconds of time duration to reach at destination, black line indicates all packets and red line indicates all errors.

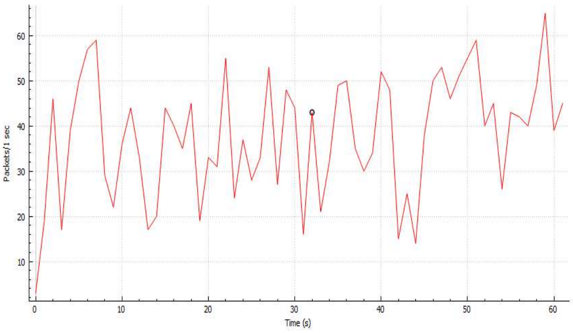


Figure 5 Illustration during the DDos attack on State Bank of Pakistan without all packets.

This graph (shown in Figure No. 5) indicates only the attack's results that are analyzed or simulated by using Wireshark and LOIC during the DDoS attack on State Bank of Pakistan. This graph is a little bit different from both, here only the level of DDoS attack is indicated via red line along with moving from source to destination with 27111 as no. of packets with 60 sec time duration to reach destination.

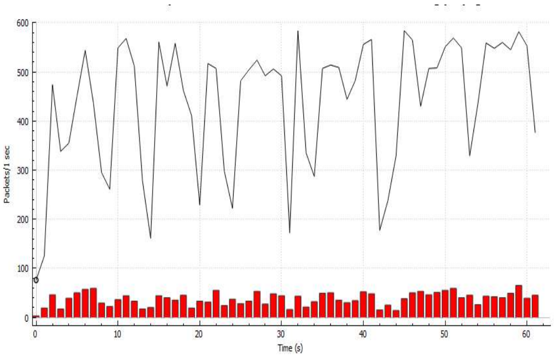


Figure 6 Illustration during the DDos attack on the State Bank of Pakistan with all packets

This graph (shown in Figure No. 6) indicates all packets with DDoS attack's results that are analyzed by using Wireshark and LOIC. This graph is compared with previous graphs because this contains the information and situation created during DDoS attack on the State Bank of Pakistan. The variation is shown in packets while moving towards the destination as compared to before DDoS attack and error ratio is increased as compared to before the attack situation. Errors vary in between 1-80 packets per second in red color bar.

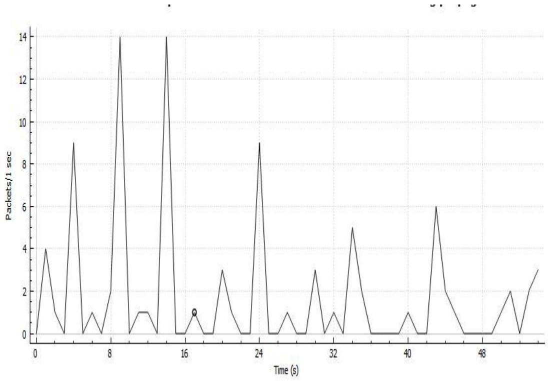


Figure 1 Illustration DDoS attack on State bank of Pakistan During Attack with TCP delay

The Graph is shown in Figure 7 illustrating the highest TCP delay in the trace file where maximum delay is traced as 14 packets per second at 9-10 and 13-15 seconds of transmission, which is a delay before getting request or delay before the finish.

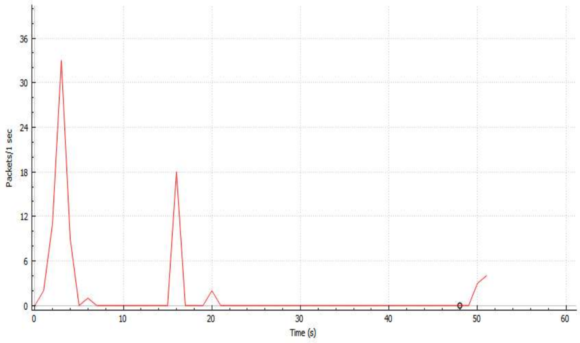


Figure 2 Illustration after the DDos attack on State Bank of Pakistan without all packets.

This graph (shown in Figure No. 8) indicates only attack's results that are conducted by using Wireshark and LOIC after the DDoS attack on State Bank of Pakistan. And 920 packets are captured in 60 sec duration. Red line show attacks.

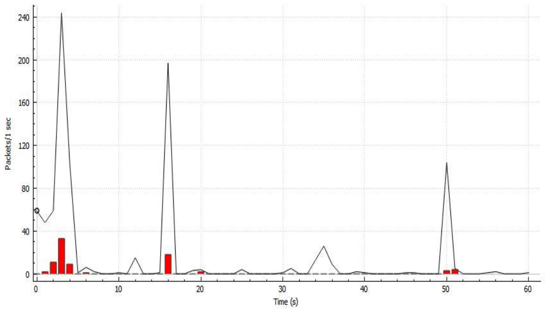
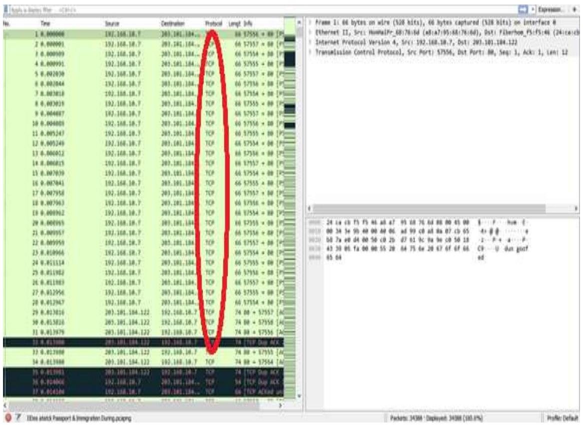


Figure 3 Illustration after the DDos attack on State Bank of Pakistan with all packets.

Figure No. 9 indicates all packets with DDoS attack's results that are conducted by using Wireshark and LOIC after the DDoS attack on State Bank of Pakistan. And 920 packets are captured in 60 sec duration. Black line indicates all packets while red bar shows all errors or cyber attacks.

5.4 Passport & Immigration

A passport is a travel document that is usually issued by the government of a country. Foreign visitors must provide their passport at the immigration checkpoints with a corresponding visa. Today, as immigration policy, it occupies a central place worldwide. Hence, Passport & Immigration is chosen to analyze the behavior. Initially, the IP address of Passport & Immigration (203.101.184.122) is used in the Wire shark tool to work in simulation environment as shown in Figure:26.



```
No.  Time      Source           Destination      Protocol Length Info
1 0.000000  192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
2 0.000001  192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
3 0.000509  192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
4 0.000991  192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
5 0.002030  192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
6 0.002044  192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
7 0.003018  192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
8 0.003019  192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
9 0.004007  192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
10 0.004009 192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
11 0.005247 192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
12 0.005249 192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
13 0.006012 192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
14 0.006015 192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
15 0.007039 192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
16 0.007041 192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
17 0.007958 192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
18 0.007963 192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
19 0.008962 192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
20 0.008965 192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
21 0.009957 192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
22 0.009959 192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
23 0.010966 192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
24 0.011114 192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
25 0.011982 192.168.10.7     203.101.184...   TCP   66 57556 → 80 [P
26 0.011983 192.168.10.7     203.101.184...   TCP   66 57557 → 80 [P
27 0.012956 192.168.10.7     203.101.184...   TCP   66 57555 → 80 [P
28 0.012967 192.168.10.7     203.101.184...   TCP   66 57554 → 80 [P
29 0.013016 203.101.184.122  192.168.10.7     TCP   74 80 → 57557 [A
30 0.013016 203.101.184.122  192.168.10.7     TCP   74 80 → 57558 [A
31 0.013979 203.101.184.122  192.168.10.7     TCP   74 80 → 57556 [A
32 0.013980 203.101.184.122  192.168.10.7     TCP   74 [TCP Dup ACK
33 0.013980 203.101.184.122  192.168.10.7     TCP   74 80 → 57555 [A
34 0.013980 203.101.184.122  192.168.10.7     TCP   74 80 → 57554 [A
35 0.013981 203.101.184.122  192.168.10.7     TCP   74 [TCP Dup ACK
36 0.014060 192.168.10.7     203.101.184...   TCP   54 [TCP Dup ACK
37 0.014104 192.168.10.7     203.101.184...   TCP   66 [TCP ACKed un
```

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: HonHaiPr_68:76:6d (a8:a7:95:68:76:6d), Dst: Fiberhom_f5:f5:46 (24:ca:cb
Internet Protocol Version 4, Src: 192.168.10.7, Dst: 203.101.184.122
Transmission Control Protocol, Src Port: 57556, Dst Port: 80, Seq: 1, Ack: 1, Len: 12
```

```
0000  24 ca cb f5 f5 46 a8 a7  95 68 76 6d 08 00 45 00   $....F.. .hvm..E.
0010  00 34 3e 95 40 00 80 06  ad 99 c0 a8 0a 07 cb 65   .4>.@.@. .......e
0020  b8 7a e0 d4 00 50 c0 2b  d7 61 9c 0a 9e c0 50 18   .z...P.+ .a....P.
0030  43 38 05 fa 00 00 55 20  64 75 6e 20 67 6f 6f 66   C8....U  dun goof
0040  65 64                                              ed
```

DDos attack Passport & Immigration During.pcapng   Packets: 34388 · Displayed: 34388 (100.0%)   Profile: Default

Figure: 10 Illustration while analyzing Passport & Immigration

Figure No. 10 shows packet capturing using Wireshark and detect source address (192.168.10.7) and destination address (203.101.184.122).

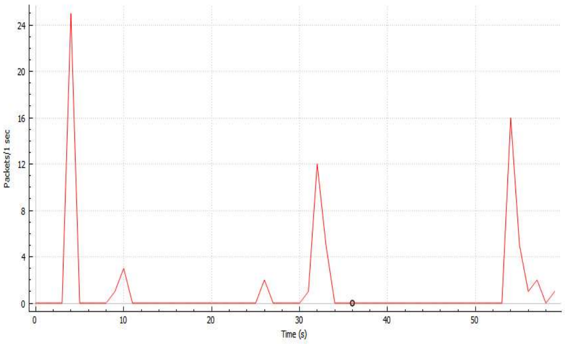


Figure: 11 Illustration before the DDos attack on Passport & Immigration without all packets.

The graph (shown in Figure No. 11) indicates DDoS attack's results those are analyzed by using Wireshark and LOIC. The above graph consists of two components such as the level of DDoS attack and the time taken to reach a destination. At initial level, before the target of DDoS attack on Passport & Immigration, we captured 1576 no of packets which are transferred in 60 seconds of time duration to reach a destination while red line indicates the level of cyber attacks.

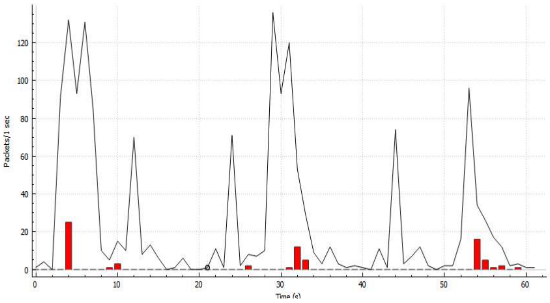


Figure: 12 Illustration before the DDos attack on Passport & Immigration with all packets.

The graph (shown in Figure No. 12) indicates all packets with DDoS attack's results that are analyzed by using Wireshark and LOIC. As compared to the above graph, this consists of three components such as packets, errors and time taken to reach a destination. Here the same 1576 no of packets are transferred in 60 seconds of time duration to reach destination, black line indicates all packets and the red line indicates all errors.

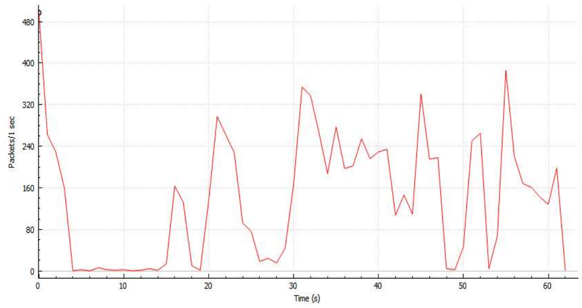


Figure 13 Illustration during the DDos attack on Passport & Immigration without all packets.

This graph (shown in Figure No. 13) indicates only attack's results that are analysed or simulated by using Wireshark and LOIC during the DDoS attack on Passport & Immigration. This graph is little bit different from both, here only level of DDoS attack is indicated via red line along with moving from source to destination with 34388as no. of packets with 60 sec time duration to reach at destination.

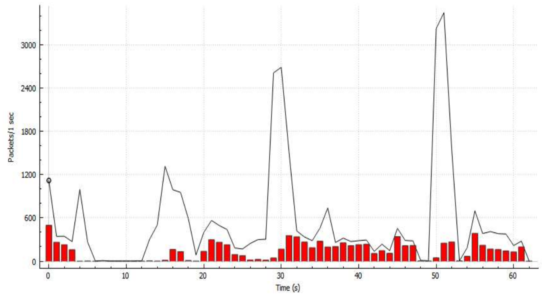


Figure 14 Illustration during the DDos attack on Passport & Immigration with all packets.

This graph (shown in Figure No. 14) indicates all packets with DDoS attack's results that are analyzed by using Wireshark and LOIC. This graph is compared with previous graphs because this contains the information and situation created during DDoS attack on Passport & Immigration. The variation is shown in packets while moving towards destination as compared to before DDoS attack and error ratio is increased as compared to before the attack situation. Errors vary in between 1-450 packets per second in red color bar.

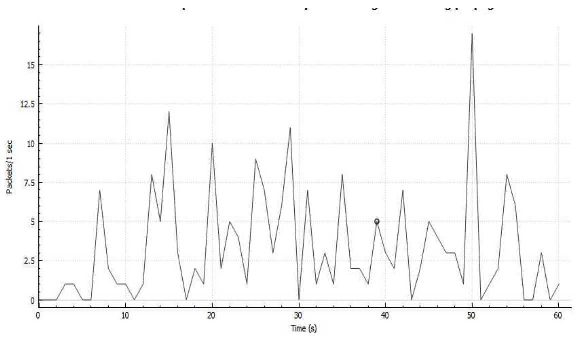


Figure 15 Illustration DDoS attack on Passport & Immigration During Attack with TCP delay

The Graph shown in Figure 15 shows the highest TCP delay in the trace file where maximum delay is traced as 18.5 packets per second at 48-52 seconds of transmission, which is delay before get request or delay before finish.

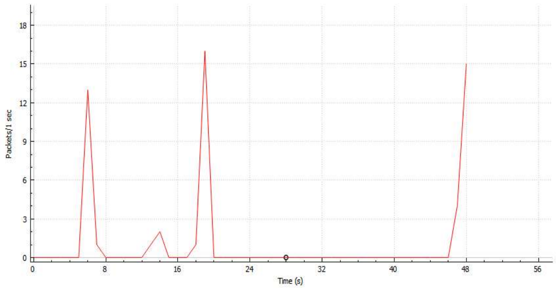


Figure 16 Illustration after the DDos attack on Passport & Immigration without all packets

Figure No. 16 indicates only attack's results that are conducted by using Wireshark and LOIC after the DDoS attack on Passport & Immigration. And 1305 packets are captured in 60 sec duration. Redline indicates cyber attacks.

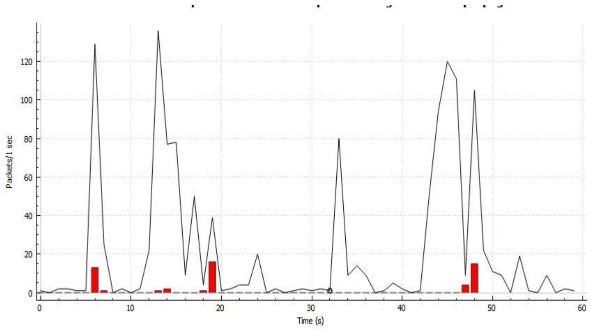


Figure 17 Illustration after the DDos attack on Passport & Immigration with all packets

This graph (shown in Figure No. 17) indicates all packets with DDoS attack's results that are conducted by using Wireshark and LOIC after the DDoS attack on Passport & Immigration. And 1305 packets are captured in 60 sec duration. Blackline indicates all packets while red bar shows all errors or cyber attacks. Table 1 show limitation and IP ,host address that are used in analysis.

Table 1 attacker IP and SERVER IP

Source IP Address	**Destination IP Address**	**IP hostname**	**Operation system**
192.168.10.13	104.17.107.192	www.sbp.org.pk	Windows 10 64-bit OS
192.168.10.13	203.101.184.122	www.dgip.gov.pk	Windows 10 64-bit OS

Table No 2 display detail about the results

Measurements	**State bank of Pakistan**	**Passport & immigration**
Packets	27111	34388
Average pps	439.7	554.2
Average packet size, B	83	86
Bytes	2240702	2943144
Average bytes/s	36 k	47 k
Average bits/s	290 k	379 k

Table No 2 display detail about the results that are capture during analyzing before, after and in during attack. The most important details among them are packet capturing during attack. This table show port and protocol that we used during the attack. We capture all these result in 60 seconds. But we can clearly analyze that packet capturing is different of all organizations.

Table 2 Measuring results

Measurements	**State bank of Pakistan**	**Passport & immigration**
Packets	27111	34388
Average pps	439.7	554.2
Average packet size, B	83	86
Bytes	2240702	2943144
Average bytes/s	36 k	47 k
Average bits/s	290 k	379 k

Table No 3 illustration detail about the result of during attack measurements. **We** analyzed in detail, the result of the two organizations of Pakistan such as State Bank of Pakistan, Passport & Immigration. SBP capture 27111 packets, Average pps 439.7, Average packet size, B 83, Bytes 2240702, Average bytes/s 36 k in almost 60 seconds, Passport & immigration capture 34388 packets Average pps 554.2, Average packet size, B 86, Bytes 2943144, Average bytes/s47 k in almost 60 seconds. We measure 2 organizations' security behavior and its clear analyze that SBP's number of packets, traffic, delay time, average pps, packet size, total bytes and bytes in second is less than other organizations. Bank attack that accord in 2018 or in this result 21 different bank effaced but SBP was secured. Its also reported that The State Bank of Pakistan (SBP) said, the banks had not been hacked. There are reports that the information of most banks has been hacked. The SBP completely rejects these reports, according to an announcement by the National Bank. This is also supported by a report from the Pakistani Computer Emergency Response Team (PakCERT) describing the timing and extent of the data leaks. Support for the SBP's complaint. As compared SBP security level is best than others. Both organizations security is very tight and secure But All measurements show that the SBP security level is more security than others.

6. CONCLUSION

As more and more people use the Internet and mobile phones, regulators need to ensure that information communication technologies (ICTs) are safe and secure from attackers. Improving and maintaining cybersecurity is becoming a serious challenge due to the complexity and limitations of human capabilities, vulnerabilities across all levels of the stack, security deficiencies, and security issues. In recent years, we have seen that cyber incidents are a significant increase in enterprise, organizations and industrial control systems (ICS). Mainly the level of cyber-attack is measured to know about the level of attack or breach or security level. DDoS attack is chosen to analyze the behavior (before the attack, during and after attack) of systems or services. This cyber-attack is targeted at the State Bank of Pakistan. DDoS attack is chosen and applied as a weapon, to analyze the behavior of systems or services. We conducted the result of a DDoS attack by using Wireshark and LOIC that help to analyses the behavior of cyber-attacks.

7. Future work

There is still a gap to understand attack and pre-requirements to secure our system and services from the attacker. Through this research, we can able to understand cyber-attack and its behavior, After detection, a mitigation procedure can be attracted immediately to filter or limit cyber-attack traffic. This research will also help other most sensitive organizations of Pakistan such as the Ministry of Interior, Federal Public Service Commission, Ministry of Finance, Revenue and Economic Affairs, Ministry of Foreign Affairs and Federal Investigation Agency. We can improve security by making our Wireshark more adaptable to classify disturbance and inconsistency configurations and change firewall rules accordingly. Adaptive systems provide faster response to malicious attacks and serious threats, including DDoS and many others.

References

[1] J. Omidosu and J. Ophoff, “A theory-based review of information security behavior in the organization and home context,” *Proc. - 2016 3rd Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2016*, pp. 225–231, 2017.

[2] S. A. Memon and J. H. Awan, “Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan,” in *Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense*, 2017, pp. 1–20.

[3] G. N. Reddy and G. J. U. Reddy, “A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies,” p. 5.

[4] K. Stojkoska, B.R., & Trivodaliev, “A review of internet of things for smart ome: challenges anf solutions,” pp. 1–2, 2016.

[5] N. Ben-Asher and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” *Comput. Human Behav.*, vol. 48, pp. 51–61, 2015.

[6] L. Montanari and L. Querzoni, “Critical Infrastructure Protection : Threats , Attacks and Countermeasures,” *Tenace*, no. March, pp. 1–164, 2014.

[7] M. AAMIR and M. A. ZAIDI, “A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques,” *Interdiscip. Inf. Sci.*, vol. 19, no. 2, pp. 173–200, 2013.

[8] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, “Cyber-attack modeling analysis techniques: An overview,” *Proc. - 2016 4th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2016*, pp. 69–76, 2016.

[9] J. A. Villaluna and F. R. G. Cruz, “Information security technology for computer networks through classification of cyber-attacks using soft computing algorithms,” *2017IEEE 9th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag.*, pp. 1–6, 2017.

[10] R. Papadie and I. Apostol, “Analyzing websites protection mechanisms against DDoS attacks,” *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-Janua, pp. 1–6, 2017.

[11] V. P. Mishra and B. Shukla, “Development of Simulator for Intrusion Detection System to Detect and Alarm the DDoS Attacks,” pp. 1–4, 2017.

[12] R. M. Yousufi, P. Lalwani, and M. B. Potdar, “A network-based intrusion detection and prevention system with multi-mode counteractions,” *Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017*, vol. 2018-Janua, pp. 1–6, 2018.

[13] J. Jang-Jaccard and S. Nepal, “A survey of

emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.

[14] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms," *Int. J. Digit. Technol. Econ.*, vol. 1, no. 2, pp. 127–134, 2016.

[15] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.

[16] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electr. Power Syst. Res.*, vol. 143, pp. 825–833, 2017.

[17] M. S. Malik and U. Islam, "Cybercrime: an emerging threat to the banking sector of Pakistan," *J. Financ. Crime*, vol. 26, no. 1, pp. 50–60, 2019.

[18] OMNISECU, "Types of Network Attacks against Confidentiality, Integrity and Avilability." 2017.

[19] X. Yan and J. Y. Zhang, "Early Detection of Cyber Security Threats using Structured Behavior Modeling," *ACM Trans. Inf. Syst. Secur.*, vol. V, no. January, 2013.

[20] M. Christodorescu and C. Kruegel, "Mining Specifications of Malicious Behavior Categories and Subject Descriptors," *6th Jt. Meet. Eur. Softw. Eng. Conf. ACM SIGSOFT Symp. Found. Softw. Eng.*, pp. 5–14, 2007.

[21] S. Jha, M. Fredrikson, M. Christodoresu, R. Sailer, and X. Yan, "Synthesizing near-optimal malware specifications from suspicious behaviors," *Proc. 2013 8th Int. Conf. Malicious Unwanted Softw. "The Am. MALWARE 2013*, pp. 41–50, 2013.

[22] R. Sekar, M. Bendre, P. Bollineni, and D. Dhurjati, "A fast automaton-based approach for detecting anamolous program behaviors," *Proc. IEEE Symp. Secur. Priv.*, vol. 9, no. C, pp. 144–155, 2001.

[23] D. Gao, M. K. Reiter, and D. Song, "Gray-box extraction of execution graphs for anomaly detection," p. 318, 2005.