Towards Designing intelligent intrusion detection systems

نحو تصميم أنظمة ذكية لكشف التسلل

Assistant Prof. WISAM ALI HUSSEIN
Ministry of Education
Dr. ZAID M. JAWAD KUBBA
University of Baghdad
Dr. AMMAR AWAD
Ministry of Education

Abstract.
The growing usage of computer networks might open more malicious access to services and systems. Security systems are used mostly to protect data centers, the duty of these systems is to protect data centers from various attacks that take deferent forms day by day, Such attacks are increasing in complexity and sophistication, resulting in disruptive consequences that can compromise data integrity, confidentiality, and availability. The ability to detect and respond to such attacks is vital to conducting necessary mitigation and limiting any damage caused to data centers services. Intrusion Detection / Prevention Systems (IDSs / IPSs) are commonly deployed to monitor and discover those sophisticated attacks from endpoints of cloud networks, limiting the deployment of distributed IDSs / IPSs that correlate security event alerts.
In this worksheet, we have tried to provide a clear track to security systems, specifically intrusion detection systems (IDS). We have provided an overview of the types of security systems, what is their function and the most important differences between them, as well as their location within the network. When we want to design these systems, it is very important to know their structure and the available types. Among them, one of the most important functions of intrusion detection systems is protection from cyber-attacks, so through our research we explained in detail the most important attacks that data centers could be exposed to and their methods of work. At the end of the worksheet, we hope that we have provided a clear idea of detection systems and how to design them.
قد يؤدي الاستخدام المتزايد لشبكات الحاسوب إلى فتح المزيد من الوصول الخبيث إلى الخدمات والأنظمة. تُستخدم أنظمة الأمان في الغالب لحماية مراكز البيانات، وتتمثل مهمة هذه الأنظمة في حماية مراكز البيانات من الهجمات المختلفة التي تتخذ أشكالًا مختلفة يومًا بعد يوم ، وتتزايد هذه الهجمات في التعقيد والتعقيد ، مما يؤدي إلى عواقب مدمرة يمكن أن تعرض سلامة البيانات للخطر، تعد القدرة على اكتشاف مثل هذه الهجمات والرد عليها أمرًا حيويًا لإجراء التخفيف الضروري والحد من أي ضرر يلحق بخدمات مراكز البيانات. يتم نشر أنظمة كشف / منع التطفل (IDSs / IPSs) بشكل شائع لمراقبة

واكتشاف تلك الهجمات المعقدة من نقاط نهاية الشبكات السحابية، مما يحد من نشر IDSs / IPSs الموزعة التي تربط تنبيهات الأحداث الأمنية.

في ورقة العمل هذه حاولنا تقديم مسار واضح عن انظمة الحماية، وبالتحديد نظم كشف التسلل، فقد قدمنا نبذة عن انواع انظمة الحماية، ما وظيفتها واهم الفروقات بينها، فضلا عن موقعها داخل الشبكة، وعندما نريد تصميم تلك النظم فمن المهم جدا التعرف على هيكليتها والانواع المتوفرة منها، من اهم الوظائف لأنظمة كشف التسلل هو الحماية من الهجمات السيبرانية، لذا ومن خلال بحثنا هذا شرحنا بالتفصيل، اهم الهجمات التي من الممكن ان تتعرض لها مراكز البيانات واساليب عملها، في نهاية ورقة العمل نتمنى اننا قدمنا فكرة واضحة عن انظمة كشف وكيفية تصميمها.

1. Introduction.

The increased use of computer networks could make it easier for hackers to access systems and services. Data centers are frequently protected by security systems, which have the responsibility of guarding against diverse threats that come in a variety of ways every day. These attacks are becoming more sophisticated and complicated, which has disruptive effects that may jeopardize the availability, confidentiality, and integrity of data. For appropriate mitigation to be carried out and any harm to data center services to be minimized, the capacity to recognize and react to such attacks is essential.. To monitor and identify those sophisticated attacks from endpoints of cloud networks, intrusion detection and intrusion prevention systems (IDS/IPS) are frequently used, restricting the use of distributed IDS/IPS that correlate security event warnings.

2. Security Systems.

It is used to monitor network traffic and detect suspicious activities, and then alert the network administrator about all abnormal, strange and malicious traffic cases, in order to prevent such traffic and take the appropriate action against it, in order to maintain the security of the network and the flow of traffic in it.

2.1 Types of security systems.

1- Intrusion Detection System (IDS).
2- Intrusion Prevention System (IPS).
3- Firewalls.

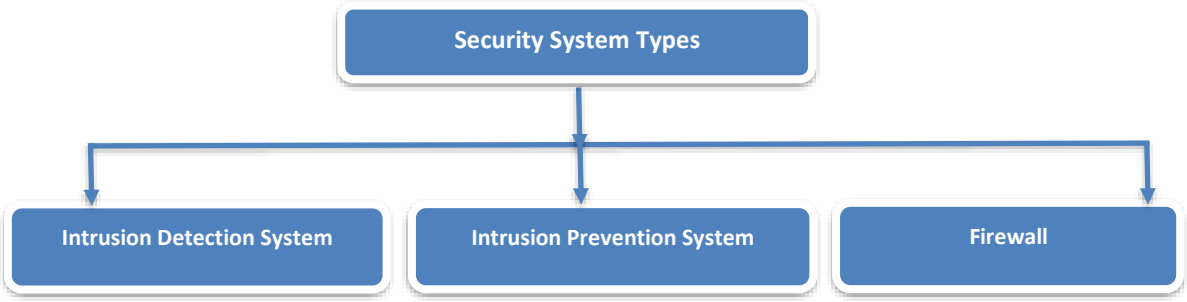

Figure (1) show security system types.

2.2 What is the difference between IDS, IPS, Firewall?

A firewall is defined as a system that is installed on a computer, or a hardware device that is placed at the forefront of a network connection to the Internet. Trying to access the device via the Internet.

The firewall monitors all network traffic and prevents unwanted traffic, by preventing a specific IP's from entering or exiting the network, or preventing a specific Port from accessing the network (that is, the function of the firewall is to determine who will communicate with the connected device or network With it and what are the allowed ports, as well as traffic routing operations or determining the nature of the Connections), from this we conclude that the work of the firewall will be limited to the third network layer or the fourth transport layer of the network layers.

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

for the Intrusion Prevention System (IPS), it is a system or device whose function is to penetrate packets and traffic and search for viruses, worms, spyware, and others. Its strength lies in its access to the first physical layer of the network layers.

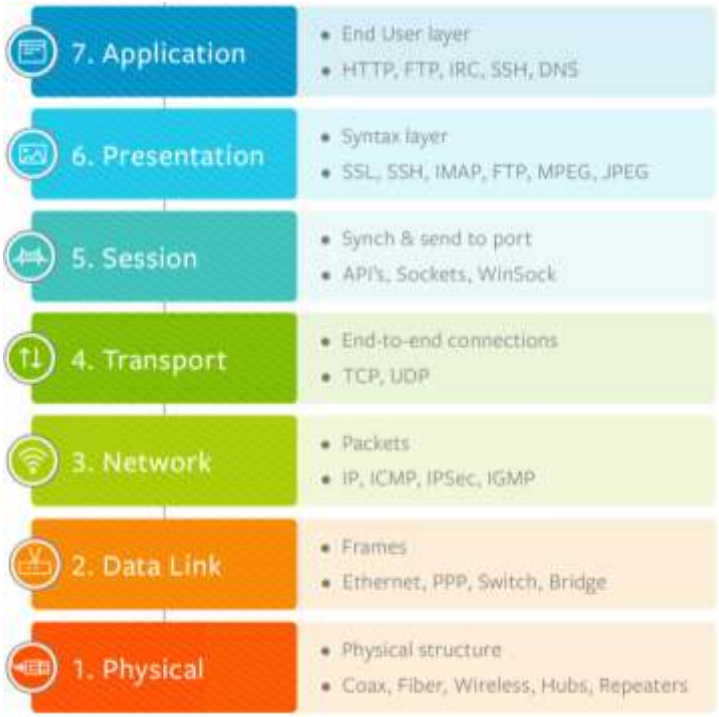

Figure (2) shows Network layers.

2.3 Where are they located on the net?

The Firewall must be placed at the front of the network to filter all malicious and suspicious traffic and not allow it to access the network. As for the IPS, it must be placed after the Firewall so that the IPS is not overburdened, and the network performance is increased.

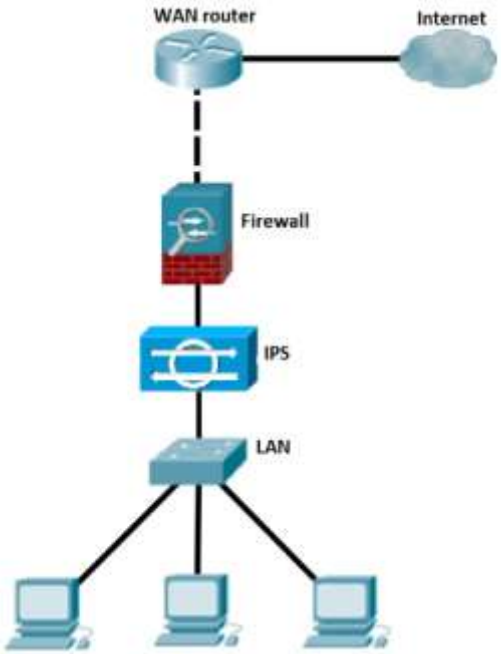

Figure (3) shows firewall and IDS location.

3. Intrusion Detection System (IDS) architecture.

Regardless of the type of IDS, the basic architecture of IDS consists of four steps. The network packets are captured using network sensors or network sniffing tools. The captured data is then filtered and examined. The filtering is performed based on filtering rules, and then signature patterns are matched with the already available signature database. An alert is generated by the IDS when a match is found with the stored signature database. The evaluation of an IDS model can be performed by implementing Machine Learning (ML) and Data Mining (DM) techniques to classify the network traffic into benign and malicious traffic flow.

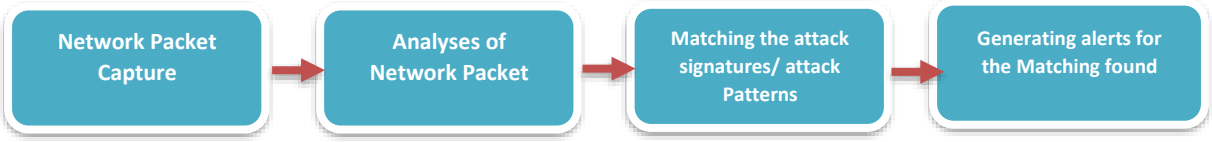

Figure (4) shows IDS architecture.

3.1 Types of intrusion detection systems.

There are five types of intrusion detection systems, they are:

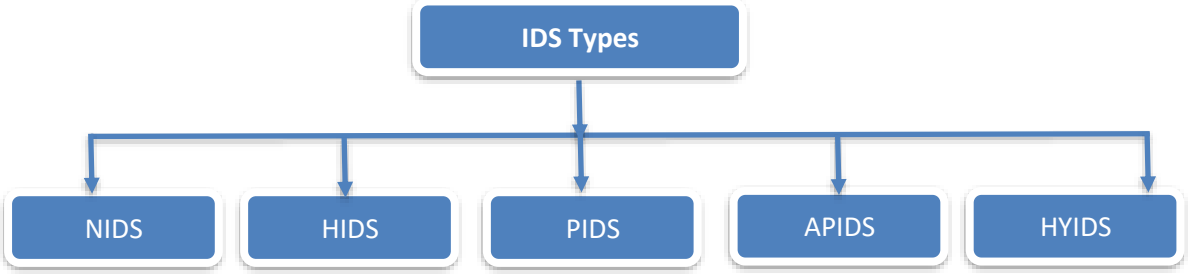

Figure (5) shows IDS types.

1- Network Intrusion Detection System (NIDS).
2- Host Intrusion Detection System (HIDS).
3- Protocol Based Intrusion Detection System (PIDS).
4- Application Protocol Based Intrusion Detection System (APIDS).
5- Hybrid Intrusion Detection Systems (HYIDS).

4. What is a cyber-attack?

A cyberattack is a deliberate act by one or more cybercriminals to steal data, fabricate information, or disrupt the digital systems of individuals or entire organizations. Through cyber security attacks, cybercriminals gain illegal and unauthorized access to one or more computers to be used later according to their criminal goals.

To deal with different types of cyber-attacks, organizations require cyber security experts and specialists.

4.1 Types of cyber-attacks that can be detected by intrusion detection systems.

Various studies have shown the diversity of cyber-attacks in cybersecurity, as well as the existence of continuous attempts by cybercriminals to develop methods of cyberattacks to comply with any security updates made by cybersecurity experts.

Here we will mention approximately (20) of the most common types of cyberattacks discovered until 2022, as follows:

4.1.1 Phishing attacks

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

How does this type of cyber-attack happen?

This attack begins when the impersonator manages to deceive the victim, after disguising himself as a trusted entity. It sends the victim an email or text message urging them to click on a malicious link, and as soon as the recipient responds and clicks on the link, malware is installed on their device, the system freezes as part of a ransomware attack, or sensitive information of the recipient is revealed.

This type of cyber-attack can have devastating consequences for individuals, including unauthorized purchases, money theft or identity theft. As for organizations, phishing is often used to gain a foothold in organization or government networks as part of a larger attack, such as an advanced persistent threat (APT) event, in which case employees are hacked to bypass the organization's security limits or distribute software. malicious software within a closed environment or obtain permission to access protected sensitive organization data.

An organization that is subject to such an attack usually suffers huge financial losses in addition to a decrease in its market share and loss of reputation and trust of its customers. Depending on the scope of this attack, the phishing attempt may escalate into a security incident for the organization that puts it in a difficult situation from which it may not find the ability to recover.

4.1.2 SPEAR PHISHING

Spear phishing is a scam that also takes place via email or communications, and targets a specific individual, organization or company. Although cyber criminals often seek to steal data for malicious purposes, they may also be known to install malware on a victim's computer.

How does this type of cyber-attack happen?

An email arrives to the victim and appears to be from a trusted source, but instead leads the recipient to a fake website full of malware. These emails often use clever tactics to get the victims' attention.

For example, there are many types of messages that appear to be sent from trusted entities but are in fact fake messages aimed at penetrating the devices of their users, such as messages that may appear to be sent from banks, or from telecommunications companies, and other national institutions.

4.1.3 Whale phishing attacks.

Whaling is a term used to describe a phishing attack that specifically targets access to sensitive and confidential information of wealthy, powerful, or prominent individuals (for example, the CEO of a company). If an individual becomes a victim of a phishing attack of this type, it can be considered a “big phishing” or what is called, a “whale”.

What does this attack have to do with phishing attacks?

Cybersecurity whaling is a subset of phishing attacks that use a specific targeting method, created by cybercriminals to impersonate a specific member of a company or organization. The attackers target the companies involved to steal confidential information or convince the victim to send money or gift cards to the impersonator.

4.1.4 DRIVE-BY ATTACKS.

A drive-by attack refers to a cyber-attack caused by a malicious script, by which a program downloads and installs itself on a victim's device, without their explicit permission.

This type of cyber-attack can happen on any user device running any operating system, and these attacks often occur when the user navigates to and browses a hacked web page.

Drive-by attacks are designed to infect devices, steal information, or cause data corruption, which often uses exploit kits to initiate automatic downloads.

What are Exploit Kits?

They are malicious pieces of software, created by hackers to identify vulnerabilities in a device, web browser, or web-based application. These vulnerabilities are then used to initiate the automatic download process and carry out the attack.

4.1.5 Ransomware

Ransomware is one of the most dangerous cyber-attacks at this time, which manages to put the sensitive information of individuals and organizations at risk.

In this type of attack, the victim is forced to delete all the necessary information from their system if they fail to pay a ransom within the timeline given by the cybercriminals, as they often blackmail the user by publishing their important files if the ransom is not paid.

4.1.6 Password attack.

In this type of cyber-attack, the attackers try to hack into different accounts of the victims by hacking their personal files and passwords giving them illegal access to all the victim’s information to be used by the attackers to achieve their goals of data theft, phishing or introducing malware on the networks.

Experts say that despite the ease and possibility of mitigating these attacks, many organizations do not implement safeguards and protections properly.

4.1.7 Eavesdropping attacks.

An eavesdropping attack, also known as a sniffing attack or snooping, is the theft of information, which is transmitted over a network by a computer, smartphone or other device connected to the Internet.

This type of cyber-attack takes advantage of unsecured network connections to access data while it is being sent or received by its user over the network in order to steal it.

How can we prevent this type of cyber-attack?

Eavesdropping attacks can be prevented in several ways, including:

- Use a personal firewall.
- Keep anti-virus software updated.
- Using a Virtual Private Network (VPN)
- Avoid public wi-fi networks.
- Adopt strong passwords.

4.1.8 Malware attacks.

A malware attack is a type of malware designed to cause harm or damage to a computer, server, client, or network without the end user's knowledge.

Online attackers create, use, and sell malware for many different reasons, but most often it is used to steal personal, financial, or business information. Although their motives differ, attackers always focus their tactics, techniques, and procedures on gaining access to privileged credentials and accounts to carry out their objective.

4.1.9 Trojan Horse

It is a type of malware that is usually disguised as an email attachment or a free download file, and then transmitted to the user's device. Once downloaded, the malicious code will perform the task it was designed for, such as backdooring into corporate systems, spying on users' online activity, or stealing sensitive data.

Indications of Trojan horse activity on the device include unusual activity such as changing computer settings unexpectedly.

4.1.10 MAN-IN-THE-MIDDLE ATTACKS

A Man-in-the-Middle attack is a type of eavesdropping attack, in which attackers interrupt an existing conversation or transmission of confidential data between two parties.

How does that happen?

After gaining entry to the "middle" of the transfer, the attackers pretend to be legitimate participants. This enables attackers to intercept information and data from any party with the intent of stealing confidential information and inflicting damage by sending malicious links or other information to each of the legitimate primary participants in a manner that may not be discovered until it is too late.

There are several common man-in-the-middle attack acronyms, including MITM, MitM, and MiM.

4.1.11 Denial of Service (DOS) Attacks and Distributed Denial of Service (DDOS) Attacks

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable. A distributed denial of service (DDoS) attack is a DoS attack that uses multiple computers or devices to flood a target resource.

Both types of attacks flood a server or web application with the intent of interrupting services, and because the server is flooded with more (TCP/UDP) packets than it can handle, it may crash, data may become corrupted, resources may be misdirected or even exhausted to the point of crippling the system.

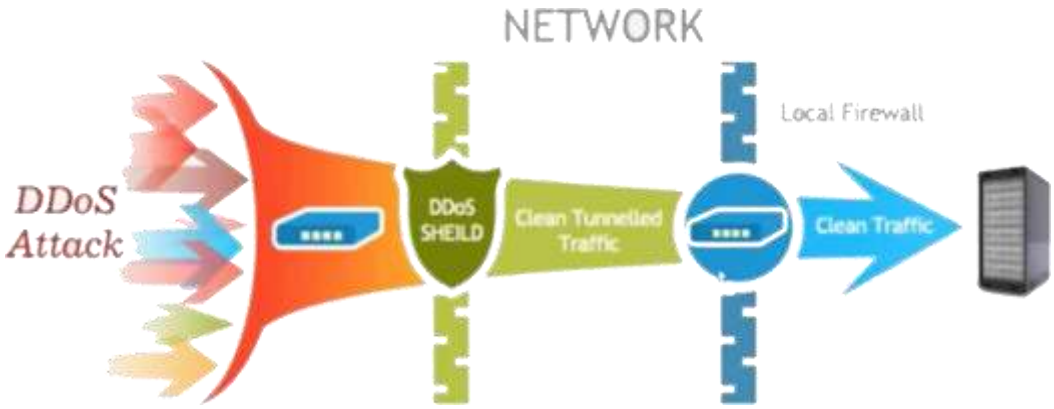

Figure (5) shows DDOS attack architecture.

4.1.12 URL Manipulation

URLs are not just addresses for browsers and servers to use as users navigate from one page to another using links, they are requests from the browser to the server that act as a form of low-level programming. When the browser requests an X from the server, the server responds with a Y.

Furthermore, there is nothing to prevent users from entering other "commands" into the browser bar to see what the server will return to them.

By manipulating certain parts of the URL, a hacker can switch to web pages that they are not supposed to have access to. URL tampering is one of the easiest attacks to perform, which can be carried out by attackers or hackers looking for vulnerabilities.

4.1.13 DNS TUNNELING ATTACK.

A hard-to-detect attack that directs DNS requests to the attacker's server, providing the attackers with a secret command-and-control channel and path to filtering data.

Attackers use the DNS tunnel to get data through firewalls. A DNS tunnel encodes command and control (C&C) messages or small amounts of data into unobtrusive DNS queries and responses. Because DNS messages can only contain a small amount of data, any commands must be small, and the data is extracted slowly. This technology is difficult to detect because DNS is a noisy protocol, making it difficult to distinguish a normal host query and normal DNS traffic from malicious activity.

4.1.14 Session hijacking attack.

A Session Hijacking attack exploits a web session control mechanism, which is usually managed by a session token.

This type of cyber-attack follows a method of hijacking a web user's session by surreptitiously obtaining the session ID and masquerading as the authorized user.

Once the user's session ID is accessed, the attacker can masquerade as that user and do whatever the user is authorized to do on the network.

4.1.15 Brute Force attack.

In this type of cyberattack, attackers try different combinations of usernames and passwords until they find one that works. The attacker might guess the key that is usually generated from the password using a key derivation function. This is known as a global search. key.
Experts recommend brute force phishing and neutralization because once attackers gain access to the network, it will be much more difficult to catch them.

4.1.16 Cross-site scripting attacks

It is a type of injection, in which malicious scripts are injected into benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end user. Flaws that could allow these attacks to succeed must always be explored, as they can occur anywhere a web application uses input from the user, processes it, and generates output directly for it without validation or encryption.

4.1.17 SQL INJECTION

An SQL injection attack consists of injecting or "injecting" a SQL query through input fields from the client into the application to affect the execution of predefined SQL commands.
An attacker using this method, if successful, can read sensitive data from the database, modify the database data (insert/update/delete), perform management operations on the database (such as shutting down the DBMS), restoring the content of a specific file contained in the DBMS and in some cases issue commands to the operating system.

4.1.18 Threats from within.

Many types of cyber-attacks happen every day, and the most shocking fact is that most of the time, there is an insider involved in the process to help the cyber criminals get information about their organization, and this is done by providing those criminals with all the information necessary to gain access, which leads to to catastrophic consequences for the organization.
Insider threats are one of the common threats of cyber-attacks on banks and financial institutions.

4.1.19 Artificial intelligence attacks.

Machine learning focuses on teaching a computer to perform several tasks on its own rather than relying on humans to perform them manually. Artificial intelligence is sometimes used to hack digital systems to obtain unauthorized information, and it can also be used to steal confidential financial data.

4.1.20 BIRTHDAY ATTACKS

Christmas attacks are brute force types of cyber-attacks that aim to disrupt communication between customers and various individuals in a company starting from the CEO to its employees.
A birthday attack is a type of cryptographic attack that breaks math algorithms by finding matches in a hash function.
The method is based on the birthday theory by which the chance of two people sharing one birthday is much higher than it appears. In the same way, the chance of detecting conflicts is also higher within the target hashing function, thus enabling the attacker to find similar fragments by using a few iterations.

5. REFERENCES

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics (Switzerland), 11(1). https://doi.org/10.3390/electronics11010016

Asgharzadeh, H., Ghaffari, A., Masdari, M., & Soleimanian Gharehchopogh, F. (2023). Anomaly-based Intrusion Detection System in the Internet of Things using a Convolutional Neural Network and Multi-Objective Enhanced Capuchin Search Algorithm. Journal of Parallel and Distributed Computing. https://doi.org/10.1016/j.jpdc.2022.12.009

Chakraborti, A., Curtmola, R., Katz, J., Nieh, J., Sadeghi, A.-R., Sion, R., & Zhang, Y. (2022). Cloud Computing Security: Foundations and Research Directions. Foundations and Trends® in Privacy and Security, 3(2), 103–213. https://doi.org/10.1561/3300000028

Daoud, M. A., Dahmani, Y., Bendaoud, M., Ouared, A., & Ahmed, H. (2023a). Convolutional neural network-based high-precision and speed detection system on CIDDS-001. Data and Knowledge Engineering, 144. https://doi.org/10.1016/j.datak.2022.102130

Daoud, M. A., Dahmani, Y., Bendaoud, M., Ouared, A., & Ahmed, H. (2023b). Convolutional neural network-based high-precision and speed detection system on CIDDS-001. Data and Knowledge Engineering, 144. https://doi.org/10.1016/j.datak.2022.102130

Diaba, S. Y., & Elmusrati, M. (2023). Proposed algorithm for smart grid DDoS detection based on deep learning. Neural Networks, 159, 175–184. https://doi.org/10.1016/j.neunet.2022.12.011

Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., Liu, T., Wang, X., Wang, L., Wang, G., Cai, J., & Chen, T. (2015). Recent Advances in Convolutional Neural Networks. http://arxiv.org/abs/1512.07108

Gupta, N., Jindal, V., & Bedi, P. (2022). CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems. Computers and Security, 112. https://doi.org/10.1016/j.cose.2021.102499