ARCENG
INTERNATIONAL JOURNAL OF ARCHITECTURE AND ENGINEERING
ISSN
2822-6895

Article Arrival Date	Article Type	Article Published Date
26.04.2025	Research Article	20.06.2025

CYBER THREATS VERSUS DATA SECURITY: THE EFFICACY OF INTRUSION, DETECTION AND PREVENTION SYSTEMS

Moses Adeolu AGOI[1], Olayemi Grace ABIMBOLA[2], Oluwanifemi Opeyemi AGOI[3]

[1]Lagos State University of Education, Lagos Nigeria, ORCID ID: 0000-0002-8910-2876

[2]Lagos State University of Education, Lagos Nigeria, ORCID ID: 0009-0000-0139-3481

[3]Obafemi Awolowo University, Osun Nigeria.

Abstract

Data security has become a paramount concern while the protection of sensitive information is indispensable. Cyberspace (I.e, an interconnectivity between work environment, internet and the intranet) has become malicious site as data are susceptible to intrusion due to the enomerous increase in malicious activities (Paul, 2020). Intrusion, detection and Prevention systems (IDPS) is a software application or device primarily designed to identify potential incidents, reports malicious activities, and enacts preventive measures using diverse response. These technologies are growingly used to support the security of sensitive identities against threats or attacks. This paper is a mixed review on the impact of IDPS technologies on data security. The paper discusses some common causes of Cybersecurity breaches, major forms of cyber threats and IDPS data security methodologies. In order to collect relevant data for the paper work, constructive questions were formed and administered to respondents using online Google form. The responses gathered were subjected to reliability analysis. The paper concludes that the use of multiple types of IDPS technologies can help to achieve a more accurate and reliable detection and prevention against cyber threats.

Keyword: Cyber Threats, Data Security, Intrution, Detection, Prevention Systems.

ISSN
2822-6895

INTRODUCTION

The introduction of Information Technology (IT) to various human endeavors has enhance easier access to all forms of data across several divides. These data are open to intrusion through malicious activities that seeks to compromise its integrity through unlawfully access, disrupting digital operation in Cyberspace; an interconnectivity between work environment, internet and the intranet. Thus, the protection, maintenance and confidentiality of these data is very important. Cyber threats originates from various sphere including hackers, corporate spies, criminal organizations and disgruntled employees. Therefore, security response methods are needed to identifying and addressing external intrusion attempts. Intrusion, detection and Prevention systems (IDPS) is a software application or device primarily designed to identify potential incidents, reports malicious activities, and enacts preventive measures using diverse response. IDPS technologies are essentially used to support the security of sensitive identities against Cyber threats or attacks.

Common causes of Cybersecurity Breaches

Threats and vulnerabilities in network security represent the potential risks and weaknesses that malicious actors may exploit to compromise the integrity, confidentiality, and availability of data within a computer network. Understanding these threats and vulnerabilities is essential for developing effective countermeasures to protect against cyber attack. The under listed are common causes of Cybersecurity breaches. Viz:-

1. Weak Authentication:

The use of weak login mechanisms that can be easily compromised or bypass, , such as or lack of multi- factor authentication or guessable passwords, creating vulnerabilities that attackers can easily gain unauthorized access to system or data.

2. Expired Software:

Failure to promptly update software, applications, and network devices, leaving them susceptible to exploitation. Attackers often target known vulnerabilities that have not been

ISSN
2822-6895

addressed.

3. Lack of Encryption

Failing to encrypt sensitive data, both in transit and at rest, leaves it vulnerable to interception and unauthorized access. Encryption helps protect the confidentiality of data even if it falls into the wrong hands (Alkhatib et al., 2021).

4. Insecure Network Protocols

The use of protocol is lacking essential security features, such as authentication or encryption, leading to data breaches, and unauthorized access, such as using HTTP, FTP and older version of SNMP.

5. Social engineering:

The use of psychological influence on people to manipulate individuals into divulging sensitive or confidential information. This can include using tactics such as baiting, impersonation, or pretexting to deceive authorized users.

Cyber Threats

These are unruly activities carried out by malicious actors with the intent to gain unauthorized access to sensitive information, exploit vulnerabilities, or disrupt services, including attacks such as malware, ransomware and phishing. It is important to understand the various types of intrusions, so as to develop effective defense mechanisms against cyber threats. Viz:-

1. Insider Intrusions:

This involve individuals within an organization using their access privileges to carry out malicious acts, such as sabotage, theft of sensitive data, or facilitating external attacks. The individual can include employees, part time workers, or even trusted entities compromising security.

2. Unauthorized Intrusions:

This involve an attacker gaining unauthorized entry to a system or sensitive data. In this type of intrusion , the attackers exploit the weaknesses in authentication mechanisms, such as expired software, guessable passwords, or poor access controls.

3. Malware Infections:

ISSN
2822-6895

This involve the deployment of harmful or malicious software, including viruses, ransomware, worms, trojans, and spyware, to compromise systems. The intrusions can occur through the installation of compromised software, infected email attachments, or surfing on malicious websites.

4. Phishing and social engineering:

This involve the manipulation of individuals to divulge sensitive information or carry out actions that can compromise security. Attackers often gain access to credentials or exploit trust of authorized users using emails, messages, or phone calls to deceive the trusted entities.

5. Internet of things (IoT) Vulnurability:

The growing increase in the connectivity of IoT devices has introduce new attack vectors where insecure IoT devices can be compromised, leading to data breaches, unauthorized access, or disruption of services or operations.

IDPS Data Security Methodologies

Intrusion Detection and Prevention Systems (IDPS) is primarily focused on identifying potential incidents, attempting to intercept them by reporting the incidents to network security administrator. IDPS technologies uses many methodologies to detect. Viz:

1. Signature-based detection:

In this, IDPS systems examines data traffic in search of unique patterns of malicious activity, i.e, patterns that corresponds to a known type of attack, and block or alert traffic matching those signatures.

2. Anomaly-based detection:

In this, IDPS systems compare definitions of normal activity against deviant the unexpected or unusual behavior to identify significant deviations from established network profiles, reflecting potential threat.

3. Stateful protocol analysis:

In this, IDPS systems compares predetermined network to identify deviations and prevent attacks that exploit vulnerabilities in network protocols. IDPS can also use the record known authentication to define acceptable activity for specific or different classes of users.

4. Malware detection:

In this, IDPS systems compare incoming traffic to a database of known malware signatures to

ISSN
2822-6895

identify malware or detect and block anomalous behavior associated with malware activity.

5. Unauthorized access prevention:

In this, IDPS systems detect and block unauthorized access attempts, such as attempts to access restricted resources or brute-force attacks.

6. Hybrid-based detection:

In this, IDPS systems combine two or more of datasecurity methodologies. The result achieved by this methodology is better than the other because it takes advantage of the strengths of the numerous methods.

RELATED LITERATURE

Michal and Maurice (2023) points out that data security has become a paramount concern for individuals, organizations as well as governments because of the fast growing digital interconnectivity of today's world. Therefore, timely and effective responses are required to fight against and safeguard networks and data. It is therefore necessary to look for an effective way to cub malicious activity in networks or cyber space. Alamin et al. (2023) noted that appropriate decisions must be carefully made in order to choose choosing the most suitable response in certain situation which is often challenging; taking wrong responses can have severe consequences. Edet et al.(2024) emphasized that identifying which response methods can have a very significant impact on mitigating threats; hence organizations are expected to optimize resource allocation, prioritize investments, and ensure that they address the most critical security issues. To this end, the research of Ekong et al. (2023) shows that many organizations have been subjected to compliance requirements and regulations on the issue of data protection and cybersecurity. Alamin et al. (2023) opined that organizations can adopt customization has a key element in order to ensure that security measures are efficient and adaptive in the face of the numerous evolving cyber threats. According to Ekong et al. (2022), Machine learning (ML) has emerged in the field of cybersecurity as a powerful tool. The findings of the research work of Michal and Maurice (2023) made a proposal on the application of Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI) and Machine learning (ML) methods. Talukder et al. (2023) proposed the introduction of a hybrid model that combines machine learning and deep learning to increase detection and security capabilities. The research work of Abdulganiyu et al. (2023) highlighted the importance of safeguarding individuals and organizational sensitive data against potential intrusions over networks. However, the research work of Sivamohan et al. (2023) looked into the various cybersecurity faced by Industry 4.0,

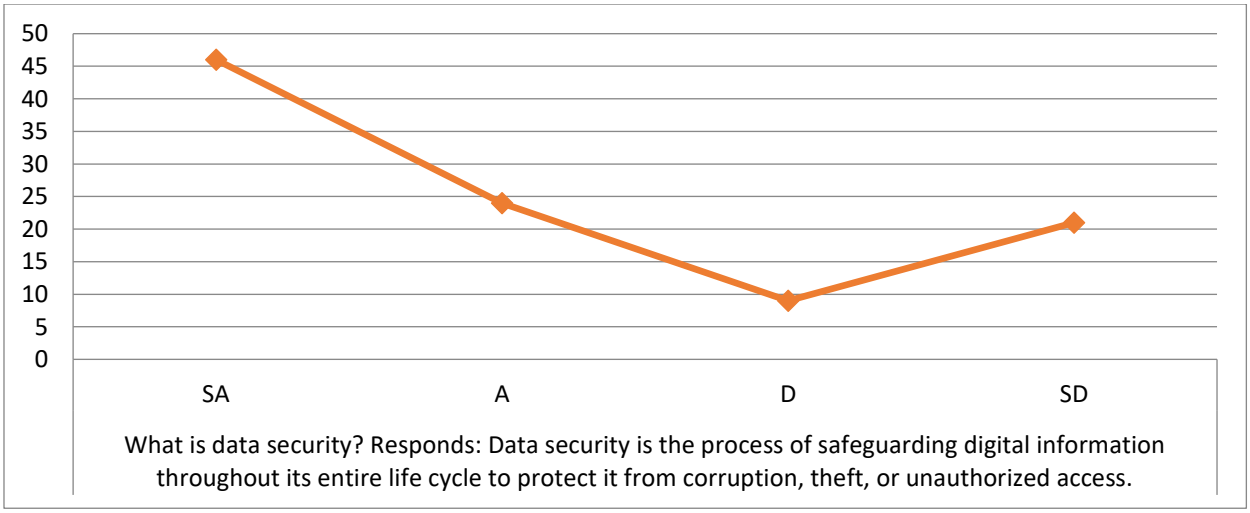
introducing real-time process monitoring and client-specific production which are susceptible to cyber threats.

MATERIALS AND METHODS

This paper combined both quantitative data (e.g., detection rates) with qualitative data (e.g., user feedback) to gain a more comprehensive understanding of the impact of IDPS technologies on data security. The researcher observed a group of security operators in their daily work to understand how they interact with IDPS technologies and address security incidents, compared the performance of various IDPS systems based on metrics like detection accuracy, false positive rate, and response time. Machine Learning (ML) was used to develop predictive models to forecast potential threats and optimize IDPS configurations. In order to collect relevant data for the paper work, constructive questions were formed and administered to security operators and IT experts using online Google form. The responses collected were subjected to Cronbach's alpha reliability analysis. The result of 0.793 gave a good reliability index of the instrument. The entire exercise took place within 46 days before completion.

RESULTS AND DISCUSSION

Analysis chart 1

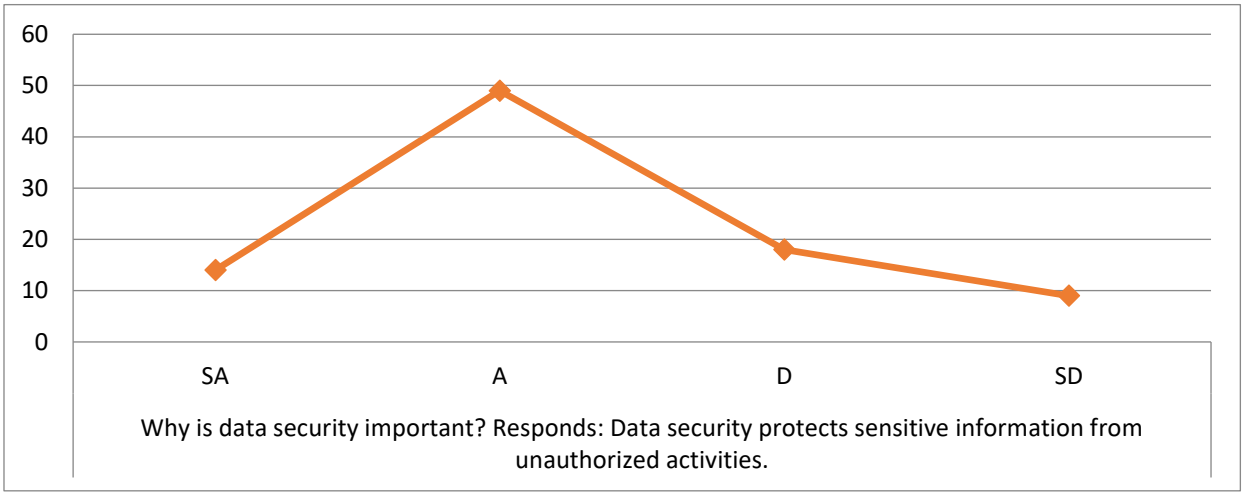


The graph plotted in chart 1 signifies that majority of the respondents fully understand the concept of data security also known as data protection. The respondents defined data security as the process of safeguarding digital information throughout its entire life cycle in order to protect it from corruption, theft or unauthorized access. According to the respondents, data security encompasses everything, including software, hardware, user devices, and storage devices; administrative and access controls; and organizations' procedures and policies. The

ISSN
2822-6895

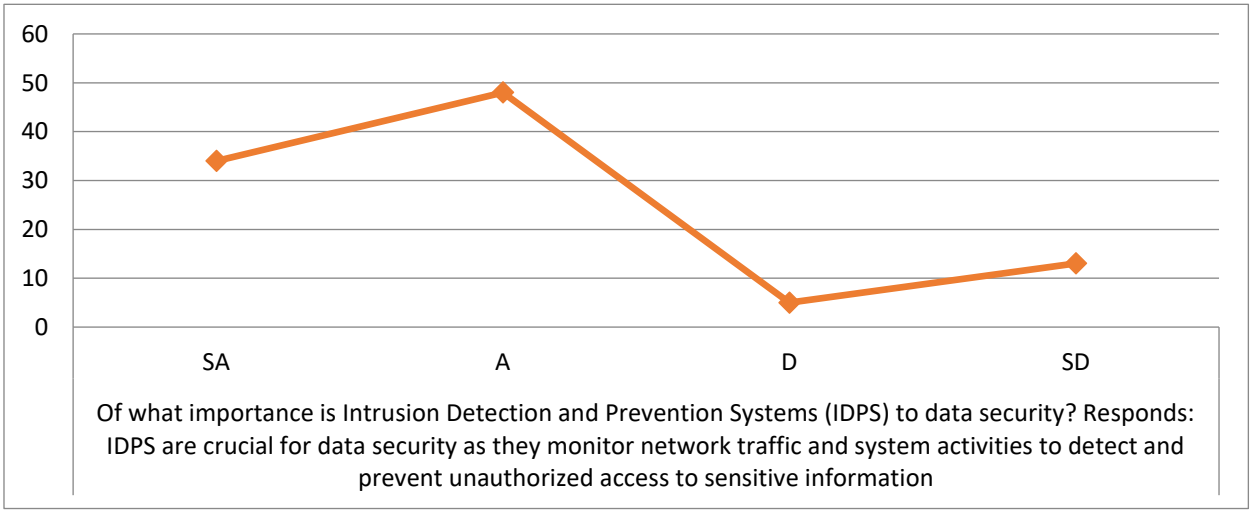
respondents explained further that data security covers all the practices and measures used to safeguard digital information from unauthorized access, inspection, recording, disruption, disclosure, modification, or destruction, in order to ensure confidentiality, integrity, and availability which are the fundamental principles data security.

Analysis chart 2



The graph plotted in chart 2 depicts that a huge number of respondents cuncur with the statement that Data security is aimed at the protection of sensitive information from unauthorized access, inspection, recording, disruption, disclosure, modification, or destruction, as earlier stated. According to the respondents, the goal of data security is to ultimately ensure the privacy and safety of sensitive data such as financial records. customer account details, or intellectual property.

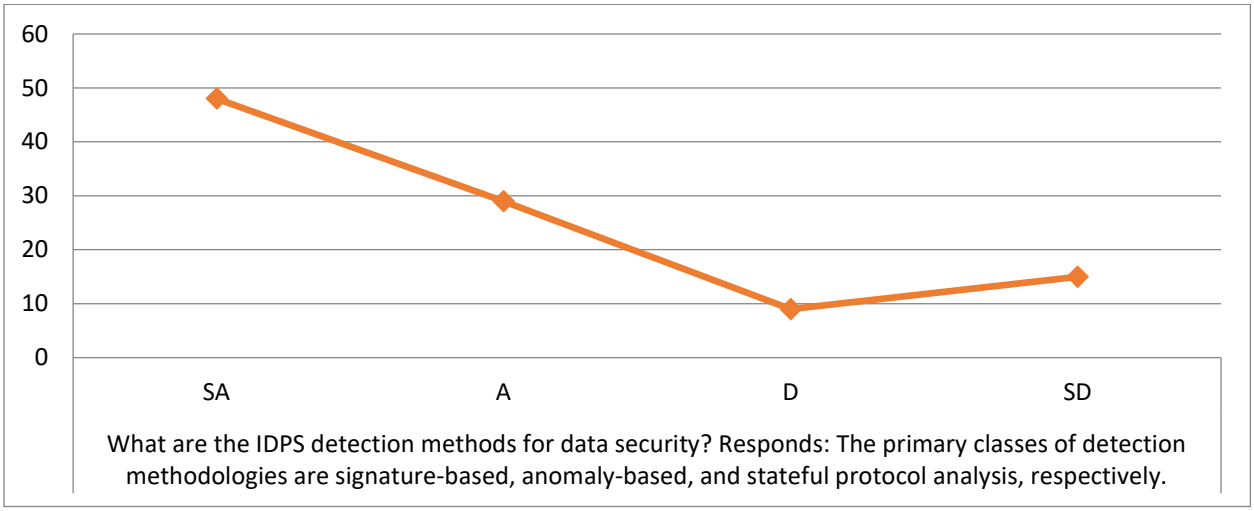
Analysis chart 3



The graph plotted in chart 3 indicates that a greater amount of respondents agree with the

statement that Intrusion Detection and Prevention Systems (IDPS) are crucial for data security as they monitor network traffic and system activities to detect and prevent unauthorized access to sensitive information. The respondents emphasized that intrusion detection and prevention system (IDPS) are network monitoring strategies that are wired to actively monitor traffic and passively block malicious activities. In other works, the respondents inferred that an intrusion detection and prevention systems (IDPS) are targeted toward the monitoring of network for threats and taking action against the threats that are detected.

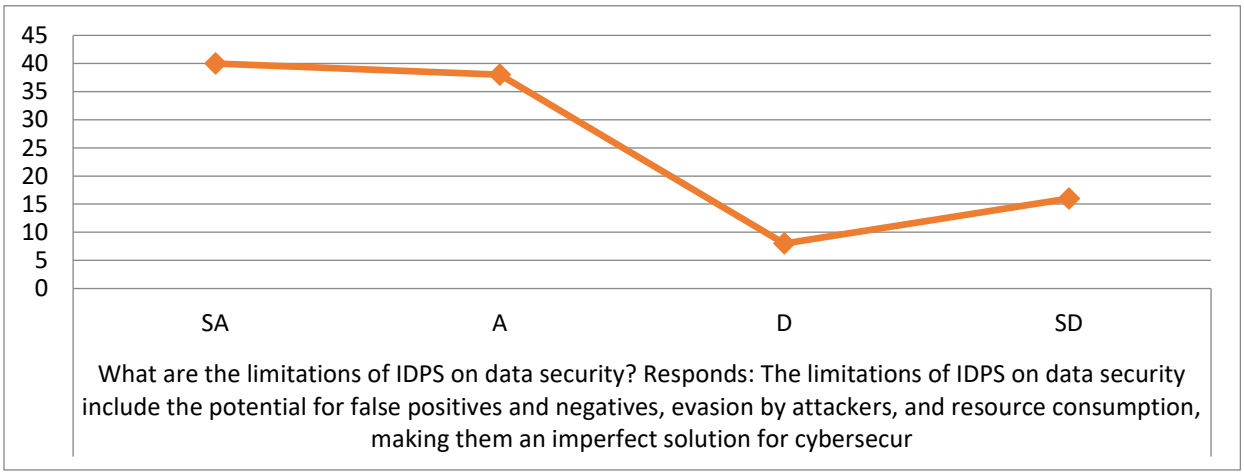
Analysis chart 4



The graph plotted in chart 4 reveals that a greater number of respondents mentioned that the primary classes of detection methodologies include signature-based, anomaly-based, and stateful- protocol analysis, respectively. The respondents added that most IDPS technologies use multiple methodologies, which may be integrated or separately, so as to effectively provide accurate and broad detection.

ISSN
2822-6895

Analysis chart 5



The graph plotted in chart 5 shows that a higher number of respondents affirmed that IDPS technologies have its limitations on data security. The respondents outlined the limitations of IDPS on data security, including evasion by attackers, potential for false positives and negatives, and resource consumption, suggesting that the technologies are not the perfect solution for data security.

CONCLUSION

This paper is focused on data security using Intrusion, detection and Prevention systems (IDPS) technologies. The paper discusses some common causes of Cybersecurity breaches, major forms of cyber threats and IDPS data security methodologies. The paper asserts that security is the concerns of individuals, organizations as well as governments as data security is paramount while the protection of sensitive information is very important, therefore, multiple types of IDPS technologies can be very helpful in monitoring the events occurring in cyberspace to achieve a more accurate and reliable detection and prevention against cyber threats.

.

REFERENCE LIST

Abdulganiyu, O.H., Ait Tchakoucht, T. & Saheed, Y.K. (2023). A Systematic Literature Review for Network Intrusion Detection System (IDS). Int. J. Inf. Secur. Vol. 22. Pp. 1125–1162 (2023). https://doi.org/10.1007/s10207-023-00682-2

Alamin, T., Khondokar, F. H., Manowarul, I., Ashraf, U., Arnisha, A., Mohammad, A. Y., Fares, A., & Mohammad, A. M.(2022). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. Journal of Information Security and Applications.

Edet, A. E., & Ansa, G. O. (2023). Machine Learning Enabled System for Intelligent Classification of Host-Based Intrusion Severity. Global Journal of Engineering and Technology Advances. Vol. 16(03). Pp. 041–050.

Ekong, A., Silas, A. & Inyang, S. (2022). A Machine Learning Approach for Prediction of Students' Admissibility for Post-Secondary Education using Artificial Neural Nework. International Journal of Computer Applications. Vol. 184. Pp. 44-49.

Ekong, B., Ekong, O., Silas, A., Edet, A., & William, B. (2023). Machine Learning Approach for Classification of Sickle Cell Anemia in Teenagers Based on Bayesian Network. Journal of Information Systems and Informatics. Vol. 5(4). Pp. 1793-1808. https://doi.org/10.51519/journalisi.v5i4.629.

Michal, M., & Maurice, D. (2023). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. International Conference Knowledge-Based Organization. Vol. 29(3). Pp. 30-37.

Paul Van Oorschot (2020). Computer Security and the Internet: Tools and Jewels.

Sivamohan S & Sridhar SS (2023). An Optimized Model for Network Intrusion Detection Systems in Industry 4.0 using XAI based Bi-LSTM framework. Neural Computer Applications. Vol. 35(15). Pp. 1459-11475. Doi: 10.1007/s00521-023-08319-0. Epub 2023 Mar 10. PMID: 37155462; PMCID: PMC9999327.