

FACULTY OF COMPUTER SCIENCE & INFORMATION COMPUTING TECHNOLOGY

DEPARTMENT OF INFORMATION COMPUTING TECHNOLOGY

PROJECT PROPOSAL

**INTRUSION PREVENTION SYSTEM**

SEE YONG JUN

2290017-DCS

Report submitted in partial fulfilment of the requirements for

DIPLOMA IN COMPUTER SCIENCE

MAY 2024

**TABLE OF CONTENTS**

[ABSTRACT 2](#_Toc169333432)

[1.0 INTRODUCTION 3](#_Toc169333433)

[2.0 PROBLEM STATEMENT 4](#_Toc169333434)

[3.0 PROJECT OBJECTIVES 5](#_Toc169333435)

[4.0 PROJECT SCOPE 5](#_Toc169333436)

[5.0 PROJECT JUSTIFICATION 5](#_Toc169333437)

[6.0 PROJECT METHODOLOGY 6](#_Toc169333438)

[7.0 PROJECT TIMELINE 6](#_Toc169333439)

[8.0 CONCLUSION 7](#_Toc169333440)

[9.0 REFERENCES 8](#_Toc169333441)

# ABSTRACT

The goal of this project is to develop an IPS (Intrusion Prevention System) that moves from a software-based platform to a web-based one and improves its accessibility and usability. The system includes a strong database system to store user information and data, which allows tracking user history and enables more effective monitoring and analysis of potential security threats. Using a web-based interface, IPS provides administrators with a centralized and user-friendly platform to manage and monitor network security, providing a more efficient and proactive approach to intrusion detection and prevention.

# INTRODUCTION

The rapid growth and increasing complexity of computer networks have made them vulnerable to various types of cyber threats. Intrusion Prevention Systems (IPS) play a crucial role in detecting and preventing unauthorized access, misuse, or malicious activities within a network. Traditional software-based IPS solutions have been effective in detecting and blocking known threats, but they often lack the scalability and flexibility required to address the evolving nature of cyber threats. Moreover, these systems typically rely on manual data analysis, which can be time-consuming and prone to human error. Essentially, an Intrusion Prevention System (IPS) functions akin to a firewall, capable of identifying irregularities within the typical flow of network traffic and subsequently halting potential malicious actions [1].

To address these limitations, this project aims to develop a web-based Intrusion Prevention System that integrates a robust database system to store user information and data, enabling more efficient and proactive monitoring and analysis of potential security threats. By transitioning from a software-based to a web-based platform, the IPS will provide a centralized and user-friendly interface for administrators to manage and monitor network security. The incorporation of a database system will allow for the tracing of user history, facilitating more effective detection and prevention of intrusions.

# 2.0 PROBLEM STATEMENT

The increasing complexity and sophistication of cyber threats have posed significant challenges to traditional Intrusion Prevention Systems (IPS). Software-based IPS solutions often lack the scalability and flexibility required to address the evolving nature of these threats [2]. Additionally, these systems typically rely on manual data analysis, which can be time-consuming and prone to human error, reducing the effectiveness of threat detection and prevention.

The current system lacks a database for storing information and data. It is software-based and requires installation before use. This limitation hinders the ability to trace user history and perform comprehensive analysis of potential security threats, which is crucial for proactive and effective intrusion prevention [3].

To address these challenges, this project aims to develop a web-based Intrusion Prevention System that integrates a robust database system to store user information and data, enabling more efficient and proactive monitoring and analysis of potential security threats.

# 3.0 PROJECT OBJECTIVES

Below are the objectives for these studies:

1. To convert from software-based into web-based
2. To implement a robust database system to follow up users’ history

# 4.0 PROJECT SCOPE

The Intrusion Prevention System (IPS) program aims to develop comprehensive security solutions designed to detect, prevent and respond to threats and attacks on web applications and network infrastructure. The system incorporates threat detection algorithms, real-time monitoring and automated response mechanisms to ensure strong protection against unauthorized access, data breaches and other malicious activities. IPS also provides secure data storage capabilities, allowing users to store and manage information and data in a highly secure storage environment. This ensures the integrity and confidentiality of sensitive information while providing documentation and reporting for compliance and audit purposes.

# 5.0 PROJECT JUSTIFICATION

Below are the significances of this project to be conduct:

5.1 Secure Data Storage Solutions

IPS provides secure data storage solutions, ensuring the protection of sensitive information from unauthorized access or data breaches.

5.2 Increased Reliance on Web Applications

The growing integration of web applications into business operations and personal activities has heightened the need for robust cybersecurity measures.

5.3 Enhanced Incident Response

IPS enhances incident response capabilities by providing detailed logging and reporting features, enabling organizations to investigate and mitigate security incidents effectively.

# 6.0 PROJECT METHODOLOGY

|  |  |  |
| --- | --- | --- |
| **Phase** | **Descriptions** | **Expected Outcome** |
| Plan | Gather the requirements of this project.  Identify the software needed to deploy.  Classified the functional and non-functional requirements. | Observation on current system. |
| Design | Translating requirements into a design.  Utilizing various designs relevant to the project to assist developers in the subsequent stage.  Creating use case diagrams, activity diagrams, and data flow diagrams. | The diagrams that might being used in this project are:  1. Use case diagram.  2. Activity diagram  3. Context diagram  4. Data flow diagram  5. Entity-relationship  diagram |
| Develop | Developing this project by using HTML, CSS, JavaScript, PHP and MYSQL.  The software used are Laragon for database, VS Code for others. |  |
| Test | Several testings are carried out to ensure it fulfil  the requirements of the system. This includes:  1. Unit testing  2. Integration testing  3. System testing | Test plan and report will be export. |

# 7.0 PROJECT TIMELINE

*Table 7.1: Gantt Chart for this project*

A colorful squares on a grid

Description automatically generated

# 8.0 CONCLUSION

In today's rapidly evolving digital environment, the significance of Intrusion Prevention Systems (IPS) has never been greater. Cyber threats are becoming more advanced and pervasive, making the need for effective and reliable IPS solutions critical. A thorough examination of different Network Intrusion Detection System (NIDS) methods is essential, as it reveals their strengths, weaknesses, and prevalence through citation analysis. This is vital for grasping trends and efficacy in developing Intrusion Prevention Systems (IPS) [4]. Therefore, a robust IDPS system that can safeguard SG communications is deemed a crucial element of the modern electrical grid [5]. This not only highlights the necessity of implementing strong IPS mechanisms but also underscores the importance of ongoing research and development in this field to protect our infrastructure. Consequently, ensuring the continuous improvement and deployment of IPS technologies is paramount for maintaining the security and integrity of our increasingly interconnected systems.

# 9.0 REFERENCES

|  |  |
| --- | --- |
| [1] | Nick Ierace, Cesar Urrutia, and Richard Bassett , "Intrusion Prevention Systems," 2019. [Online]. Available: http://www.rickbassett.com/publishing/published/Intrusion%20Prevention%20Systems%20-%20June%2005.pdf. |
| [2] | Scarfone, K., & Mell, P., "Guide to Intrusion Detection and Prevention Systems (IPDS)," 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf. |
| [3] | Bace, R., & Mell, P., "Intrusion Detection Systems," 2021. [Online]. Available: https://csrc.nist.rip/library/NIST%20SP%20800-031%20Intrusion%20Detection%20Systems%20%28IDS%29,%202001-11.pdf. |
| [4] | Satish Kumar, Sunanda Gupta, Sakshi Arora, "Research Trends in Network-Based Intrusion," 22 November 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9623451. |
| [5] | Sarigiannidis, Panagiotis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8684225. |
| [6] | Khalid Khan, Amjad Mehmood, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture,* vol. 105, 2020. |
| [7] | Khraisat, A., Gondal, I, "Survey of intrusion detection systems: techniques, datasets and challenges.," *Cybersecur 2, 20,* 2019. |
| [8] | Mustafa Al Lail, Alejandro Garcia, "Machine Learning for Network Intrusion Detection - A Comparative Study," 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/7/243#metrics. |
| [9] | M. Poongodi, V. Vijayakumar, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," 4 October 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8859299. |