NIDSTOKNOW: A WEB-BASED NETWORK INTRUSION DETECTION SYSTEM (NIDS) LEARNING AND SIMULATION PLATFORM USING COWRIE HONEYPOT

A Capstone Project
Presented to the
Faculty of College of Computer Studies
Laguna State Polytechnic University
Siniloan (Host) Campus

In Partial Fulfillment of the Requirements for the Degree

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

By:

DANLIE KEN BISANA GREGORY
HANZ HENDRICK RATAC LACSI
ANGEL BLESS MARAY MENDOZA

ZERAH-JANE M. ASTOVEZA
Adviser

DECEMBER 2025

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF COMPUTER STUDIES

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

VISION, MISSION, QUALITY POLICY, CORE VALUES, COLLEGE GOALS, AND PROGRAM OBJECTIVES

VISION

LSPU is a center of technological innovation that promotes interdisciplinary learning, sustainable utilization of resources, collaboration and partnership with the community and stakeholders.

MISSION

LSPU, driven by progressive leadership, is a premier institution, providing technology-mediated agriculture, fisheries, and other related and emerging disciplines significantly contributing to the growth and development of the region and nation.

QUALITY POLICY

LSPU delivers quality education through responsive instruction, distinctive research, sustainable extension and production service. Thus, we are committed with continual improvement to meet applicable requirements to provide quality, efficient and effective services to the university stakeholder's highest level of satisfaction through an excellent management system imbued with utmost integrity, professionalism and innovation.

CORE VALUES

LSPU Develops:

Spirited **T**ransparent **U**pright **D**isciplined **E**fficient **N**oble **T**rustworthy **S**killful

COLLEGE OF COMPUTER STUDIES GOALS

The College of Computer Studies aims to develop globally competitive graduates equipped with knowledge, skills and values necessary for Information Technology Education programs in undertaking instruction, research, extension and production.

THE OBJECTIVES OF THE PROGRAM (BSIT)

The Bachelor of Science in Information Technology graduates are professionals that can adapt with the fast-paced computing trends responsive to global IT demands.

It is designed to enable students to achieve the following by the time they graduate:

1. Apply knowledge for solving computing problems employing design and development solutions for business-driven application, installation, processes, operation, maintenance and administration of IT hardware and software.

2. Utilize modern computing tools and techniques in research and development projects.
3. Communicate effectively as a member or leader of the computing society with social, moral and legal responsibilities to accomplish a common goal.
4. Engage in life-long learning as a foundation for continuing professional advancement.

Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

COLLEGE OF COMPUTER STUDIES

APPROVAL SHEET

The capstone project entitled **"NIDSTOKNOW: A WEB-BASED NETWORK INTRUSION DETECTION SYSTEM(NIDS) LEARNING AND SIMULATION PLATFORM USING COWRIE HONEYPOT,"** prepared and submitted by **DANLIE KEN B. GREGORY, HANZ HENDRICK R. LACSI**, and **ANGEL BLESS M. MENDOZA**, in partial fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**, major in **NETWORK ADMINISTRATION**, is hereby recommended for approval and acceptance.

ZERAH-JANE M. ASTO
Capstone Project Adv

==========

Approved by the Committee on Oral Examination with a grade of _____.

FIRSTNAME MI. LASTNAME, XXX
Subject Specialist

FIRSTNAME MI. LASTNAME, XXX
Technical Editor

FIRSTNAME MI. LASTNAME, XXX
Statistician

FIRSTNAME MI. LASTNAME, XXX
Language Critic

ZERAH-JANE M. ASTOVEZA
Research Coordinator

==========

Accepted and approved in partial fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**, Major in **NETWORK ADMINISTRATION.**

ARCHIEVAL M. JAIN
Associate Dean

FIRSTNAME MI. LASTNAME, XXX
Chairperson, Research and Development

_____
Date Signed

RESEARCH CONTRIBUTION NO.	

DEDICATION

Start your dedication here.

Acknowledgement and Dedication should only be limited to only one per group and should be one to two pages at most.

Mention only people who have directly been involved in the process of making the manuscript.

Slang, Tag-lish and unnecessary side comments are not acceptable.

Use the standard paragraph style. Icons, pictures and other graphics are not allowed.

It should be written in a formal style and serious tone.

ACKNOWLEDGMENT

The researchers sincerely extend heartfelt gratitude and appreciation to the following individuals who contributed to the successful completion of this study:

Zerah-Jane M. Astoveza, Capstone Project Adviser and RIU Head, for her encouragement, constructive feedback, expertise, and insightful suggestions that greatly enriched the research;

Jemar A. Banawa, Subject Specialist, for her unwavering support, concern, and valuable guidance that significantly improved this study;

Aira M. De Jesus, English Critic, for dedicating time and effort to review and refine the manuscript;

Niño Emmanuel Aldi L. Astoveza, Technical Editor, for his assistance and commitment in ensuring the technical accuracy of the manuscript;

Francis F. Balahadia, DIT, Dean, for his encouragement, concern, and continuous support that motivated the completion of this work;

The eight IT experts who generously participated as respondents, for their cooperation and contributions in fulfilling the objectives of the study;

And above all, the Almighty God, for granting wisdom, strength, hope, spiritual guidance, and motivation that sustained the researcher through the challenges encountered in making this study possible.

THE AUTHOR/S

ABSTRACT

LastName, FirstName MI. of Bachelor of Science in Information Technology, Laguna State Polytechnic University, 2022, "Title of Capstone Project", Co-Author: Name of Adviser.

The abstract should not be more than two pages long or not more than 250 words. Adopt 1.5 line spacing for the body text. It must be written in narrative form, not including tables, graphs, material references or any other unusual abbreviations. Verbs should be presented in past tense.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

DEFINITION OF TERMS

This section includes important or key terms that should be substantially and clearly define according to how they are used in the study in order to facilitate understanding of the problem and avoid ambiguous meaning to term which can be otherwise interpreted in different ways.

Operational Terms

Administrator. It is defined as the proponent who manages the technical aspects, user roles, and overall configuration of the NIDStoKnow platform.

Attacker. This pertains to the learner role that simulates intrusion attempts within the controlled environment of the system.

Defender. It denotes the learner role that uses the system's real-time detection feed and tools to implement defensive strategies.

Instructor. This is understood as the faculty member who assigns modules, monitors progress, and evaluates learner performance using the platform.

Learner. It designates the student who uses the platform to study NIDS concepts and perform simulations.

NIDStoKnow. This is characterized as the proposed web-based Network Intrusion Detection System (NIDS) learning and simulation platform using Cowrie Honeypot.

Panel. It signifies the feature in the platform (attacker, defender, or instructor) that provides tools and functions specific to each role.

Simulation. This is described as the interactive environment in the platform where attacker and defender activities are initiated and conducted.

Technical Terms

Agile Software Development. It is defined as a flexible, iterative methodology for creating software, emphasizing collaboration, adaptation, and incremental improvement.

Aho-Corasick Algorithm. This pertains to a multi-pattern string matching algorithm used in signature-based intrusion detection for identifying attack patterns.

Anomaly-Based Detection. It denotes a NIDS method that detects deviations from normal network behavior.

Cowrie Honeypot. This is understood as a medium-interaction honeypot that simulates SSH and Telnet services to record attacker activities without risking actual systems.

Honeypot. It designates a decoy computer system designed to lure attackers and log their behaviors for analysis.

Hybrid Detection. This is characterized as a NIDS method that combines signature-based and anomaly-based detection techniques for improved accuracy.

ISO/IEC 25010. It signifies the international standard software quality model used to evaluate characteristics such as functionality, usability, reliability, and security.

Learning Management System (LMS). This is described as a digital platform for delivering instructional content, assessments, and monitoring learner progress.

Linux Terminal. It is defined as a command-line interface used to execute commands and analyze system or network data.

Network Intrusion Detection System (NIDS). This pertains to a security system that monitors and analyzes network traffic to detect malicious or suspicious activities.

Regular Expression (Regex). It denotes a sequence of characters that defines a search pattern, used in text and intrusion detection.

Role-Based Access Control (RBAC). This is understood as an access control framework in which permissions are granted according to user roles within the system.

Signature-Based Detection. It designates a NIDS method that identifies malicious activity by comparing it to known attack patterns.

Isolation Forest Algorithm. This is characterized as a machine learning algorithm designed for anomaly detection, applied in NIDS to detect unusual or suspicious activity.

WebSocket. It is defined as a communication protocol that provides full-duplex interaction between client and server over a single TCP connection.

CHAPTER I

INTRODUCTION

The increasing prevalence of global cyber threats underscores the need for cybersecurity education at all levels, including within Higher Education Institutions (HEIs), as it is essential for building a more informed and secure digital society (Maraj et al., 2021). Vikram (2025) reported that the United States of America (USA), United Kingdom (UK), and Australia topped the list of the best countries to study cybersecurity. The International Business Machines Corporation (IBM) in the USA has likewise targeted 3 million individuals, including college students, by developing the Cyber Campus, a comprehensive Software-as-a-Service (SaaS) platform that simulates real-world networks and cyberattacks for training, testing, and research purposes (Koehler et al., 2024).

In contrast, inadequate cybersecurity education in developing regions, especially in Southeast Asia, creates a skills gap that hinders effective defense against rising digital security threats (Lavrova, 2025). A recent study by Dillon and Tan (2024) found that although there is strong student interest in cybersecurity, there are relatively few formal degree programs and limited access to practical, hands-on training environments in many Southeast Asian countries. This deficit in experiential learning means that learners often graduate with theoretical knowledge but limited ability to apply detection and analysis methods in realistic settings.

One of the main topics in IT courses is Network Intrusion Detection Systems (NIDS). The primary goal of NIDS is to identify malicious or suspicious logging information and report it to the network administrator (Kumar et al., 2021). Hence, it is a critical subject in cybersecurity education, as NIDS helps detect and prevent

cyberattacks. However, simulating cybersecurity activities, including NIDS, through hands-on exercises is difficult because real attacks can harm networks (Song et al., 2022) and may be challenging to understand, as many originate from Linux environments (Jain & Singh, 2011). This makes it difficult for students to visualize how NIDS functions in real-world scenarios. Even so, learning the concepts of NIDS remains essential, as it prepares students to design and manage secure networks while equipping them with the skills to address security risks effectively (Jain & Waoo, 2023).

Cowrie, a honeypot system that simulates fake Secure Shell (SSH) and Telnet services, offers a safe environment for studying attacks. It allows attackers to interact with what appears to be a real server, attempting logins or executing Linux commands, without harming actual systems (S & Chakkaravarthy, 2023). Cowrie records detailed logs of these activities, which provide valuable insights into attacker behavior and techniques (Carrillo-Mondejar et al., 2024). For example, it frequently captures brute-force attempts and reconnaissance commands such as *uname –a* that probe system information (Setianto et al., 2021).

Therefore, to address the gaps in cybersecurity education, particularly the lack of practical, hands-on experiences in understanding real-world network threats, this study proposes the development of NIDSToKnow, a web-based Network Intrusion Detection System (NIDS) learning and simulation platform using the Cowrie honeypot. This platform is designed to enhance learning by simulating three NIDS methods: signature-based, anomaly-based, and hybrid detection. By integrating Cowrie into a learning management system (LMS) framework, NIDSToKnow provides a safe and interactive environment where IT students can observe and analyze simulated attacks in a built-in Linux terminal. This simulation-based

approach not only mitigates the risks of live testing but also bridges the gap between theory and practice, thereby equipping students with practical skills for real-world cybersecurity challenges.

Project Context

In the Philippine context, challenges in cybersecurity education are evident in both global rankings and local implementation. According to the Global Cybersecurity Index (2023), the Philippines ranks 61st out of 182 countries, while in the National Cybersecurity Index (2023), it dropped to 48th from 43rd out of 195 countries. The government has responded through initiatives such as the Cybercrime Prevention Act of 2012 or Republic Act 10175 (Republic of the Philippines, 2012) and the National Cybersecurity Plan 2022 (DICT, 2022), which also mandates CHED and HEIs to integrate cybersecurity into IT and related programs. However, despite these efforts, their impact on higher education remains limited, as many HEIs still lack structured, hands-on cybersecurity learning environments that can equip students with the practical skills needed to meet industry demands.

Recognizing the growing demand for skilled professionals, the Commission on Higher Education (CHED), in collaboration with DICT, has endorsed the integration of cybersecurity education into the curricula of State Universities and Colleges (SUCs) and private institutions, particularly IT programs. This has been further supported through capacity-building activities such as webinars, seminars, and specialized training.

Another investigation on Filipinos' internet security awareness showed that while many respondents had knowledge of security tools and practices, actual implementation was low and awareness of underlying threats (e.g., phishing, malware) was limited. This gap points to the need for more structured, formal training

in cybersecurity topics (Omorog & Medina, 2020). However, many institutions still face gaps in establishing structured, hands-on learning environments that adequately prepare students for real-world cyber threats (De Ramos & Esponilla, 2022).

These concerns are not unique to the Philippines, as Xiao et al. (2023) highlighted that HEIs also face challenges in the new era, including a lack of innovation, interaction, immersion, and comprehensiveness, which mirrors the gaps observed locally.

Firstly, the lack of innovation in cybersecurity education remains a major issue. Many HEIs continue to rely on traditional methods such as lectures and seminars, without integrating modern learning theories or up-to-date industry standards. Valdez, Rivera, and Pabico (2015) noted that outdated textbooks and teacher-centered approaches often fail to address emerging cybersecurity threats, resulting in a disconnect between what is taught and what the field demands. Collaborative, practice-oriented learning is crucial in addressing these educational challenges (Mäkelä et al., 2018), and Begley et al. (2013) emphasized that practical tasks lead to better performance and retention, reinforcing that experiential activities are foundational to effective learning.

Secondly, the absence of immersive learning environments contributes to low student engagement. Rather than fostering active participation, many institutions rely heavily on theory-based instruction that leaves students in passive roles. Aquino and Noroña (2021) reported that IT students in the Philippines often experience limited exposure to laboratory-based and simulation-driven exercises, which hampers the development of applied cybersecurity competencies. Similarly, Ferm (2021) showed that bridging theory and practice through applied learning boosts students' confidence in applying skills, underscoring the importance of immersive environments.

Thirdly, there is a lack of interaction within classroom environments. Educator-dominated, hierarchical teaching models often discourage student involvement and discussion, resulting in learners struggling to internalize concepts and apply them in practice. In a local study, Manalo and Gallardo (2024) found that interactive and collaborative classroom strategies improved IT students' problem-solving and critical thinking skills, demonstrating that learner-centered methods are more effective. Additionally, Thanh (2020) highlighted that self-assessment and reflection enhance independent learning, improving students' self-esteem and engagement.

Lastly, the lack of comprehensiveness in current cybersecurity programs remains a concern. Many curricula fail to adopt prevention-oriented mindsets and often lack full-time faculty, institutional support, or innovative instructional methods such as simulations. Moldez, Crisanto, Cerdeña, Maranan, and Figueroa (2024) demonstrated that incorporating innovative learning strategies in Philippine higher education improves student engagement and understanding, while project-based learning has also been shown to foster motivation by connecting classroom activities to real-world cybersecurity problems (Tsoy et al., 2023).

One HEI in Laguna offers IT majors, particularly in Network Administration. Despite offering this specialization, proponents found out in interviews that students face a lack of hands-on activities, especially in areas like NIDS, which is a key topic in their curriculum. Four out of five interviewed third-year Network Administration students admitted that they do not have enough knowledge about NIDS particularly in its three methods: signature-based, anomaly-based, and hybrid. Asif et al. (2013) said that NIDS is one of the most important areas in the field of computer networking. The first respondent suggested that an educational system focusing on NIDS would be a

big help. The second interviewee also expressed a lack of awareness and emphasized the need to develop more learning and simulation tools about NIDS. In a study authored by Kumar et al. (2021), they listed popular and effective NIDS tools such as the Snort, Suricata, OSSEC, and etc. that use different methods. The third student had a general understanding that NIDS is a tool used to detect malicious website activities but was unfamiliar with its specific methods, also highlighted the need for real-life configuration experiences. The fourth student showed confusion between NIDS signatures and personal digital signatures and had not encountered any NIDS tools yet. The fifth respondent shared that she only had limited knowledge and suggested a dedicated learning system to improve awareness.

For the interviewed fourth-year Network Administration students, while all five claimed some familiarity with NIDS, their level of understanding still varied. AlSanad (2024) emphasized that cybersecurity education is a vital topic that requires a lot of attention and thought. Students should be systematically taught about the importance of cybersecurity and how to prevent cyber-attacks. The first student explained that NIDS could detect and block visitors based on their IP address once they access a website, but still lacked a clear understanding of the detailed mechanisms behind it. The second respondent was somewhat familiar but only understood the hybrid method as a combination of the signature and anomaly approaches. The third interviewee, although aware of NIDS from earlier studies, felt the topic was not explained in-depth and that their curriculum focused more on firewalls. The fourth student acknowledged the general purpose of NIDS but admitted not being fully familiar with how it works or the specific methods used. The fifth respondent had prior experience using Snort, though this was outside the academic setting. All respondents recommended that a more focused, practical approach to

teaching NIDS would improve their understanding in real-world network security. As Aoyama et al. (2024) emphasized that practical, exercise-based education combining lectures with hands-on training enhances cybersecurity understanding like the project proposal NIDStoKnow, a web-based learning and simulation platform that teaches NIDS using the Cowrie honeypot.

Research Objectives

General Objectives

To design and develop a web-based platform entitled "NIDSToKnow: A Web-Based Network Intrusion Detection System (NIDS) Learning and Simulation Platform Using Cowrie Honeypot".

Specific Objectives

1. To design and develop a web-based Network Intrusion Detection System (NIDS) Learning and Simulation Platform Using Cowrie Honeypot with the following features:
    1.1. Theoretical activities focused on NIDS methods and interactive simulation to demonstrate detection approaches.
    1.2. To provide a practical simulation using the Cowrie honeypot to detect and analyze malicious activities in an attacker–defender setting.
    1.3. To provide instructors with tools to assign modules, monitor learner engagement, and deliver feedback.
2. To utilize different algorithms for detection with NIDS methods:
    2.1. Aho-Corasick Algorithm (ACA) for signature-based detection
    2.2. Isolation Forest Algorithm (IFA) for anomaly-based detection

2.3. Combination of ACA and IFA for hybrid detection

3. To implement Role-Based Access Control (RBAC) for learners, instructors, and administrators to manage access to platform features based on user roles.

4. To evaluate the software quality using ISO25010.

Conceptual Framework

The NIDStoKnow is an online platform developed to offer a comprehensive and interactive learning experience to learners who are interested in learning and researching NIDS. The system is designed to cater three different users: students, instructors, and administrators. Each user has their own roles and responsibilities that support the overall operation of the system. To strengthen the learning experience, the system also integrates the Cowrie honeypot, which collects real attack data, and uses the Aho-Corasick and Isolation Forest algorithms as part of its detection engine. All essential data, including user profiles, modules, logs, and results, are securely stored in a central database.

Once users interact with the platform, students gain access to the LMS, where they can study modules, take quizzes, and join practical exercises. They may also participate in simulation activities where they assume the role of attacker or defender in realistic cyberattack scenarios. Teachers guide and monitor this learning process by assigning modules, managing simulations, and providing feedback on performance. Administrators ensure smooth system operation by managing user access, updating detection signatures, and configuring system settings. At the core, the detection engine processes simulation and honeypot data using both signature and

anomaly-based techniques, generating accurate results that are displayed in real time through dashboards, notifications, and alerts.

As a result of these processes, the platform establishes an interactive and efficient learning environment. It enables students to develop both theoretical understanding and practical competence in NIDS. Likewise, instructors are supported in delivering lessons more effectively through the use of guided simulations, while administrators ensure that the system remains secure, updated, and properly managed. In its entirety, the platform functions as a comprehensive tool that addresses the gap between classroom-based instruction and real-world applications in the field of cybersecurity.

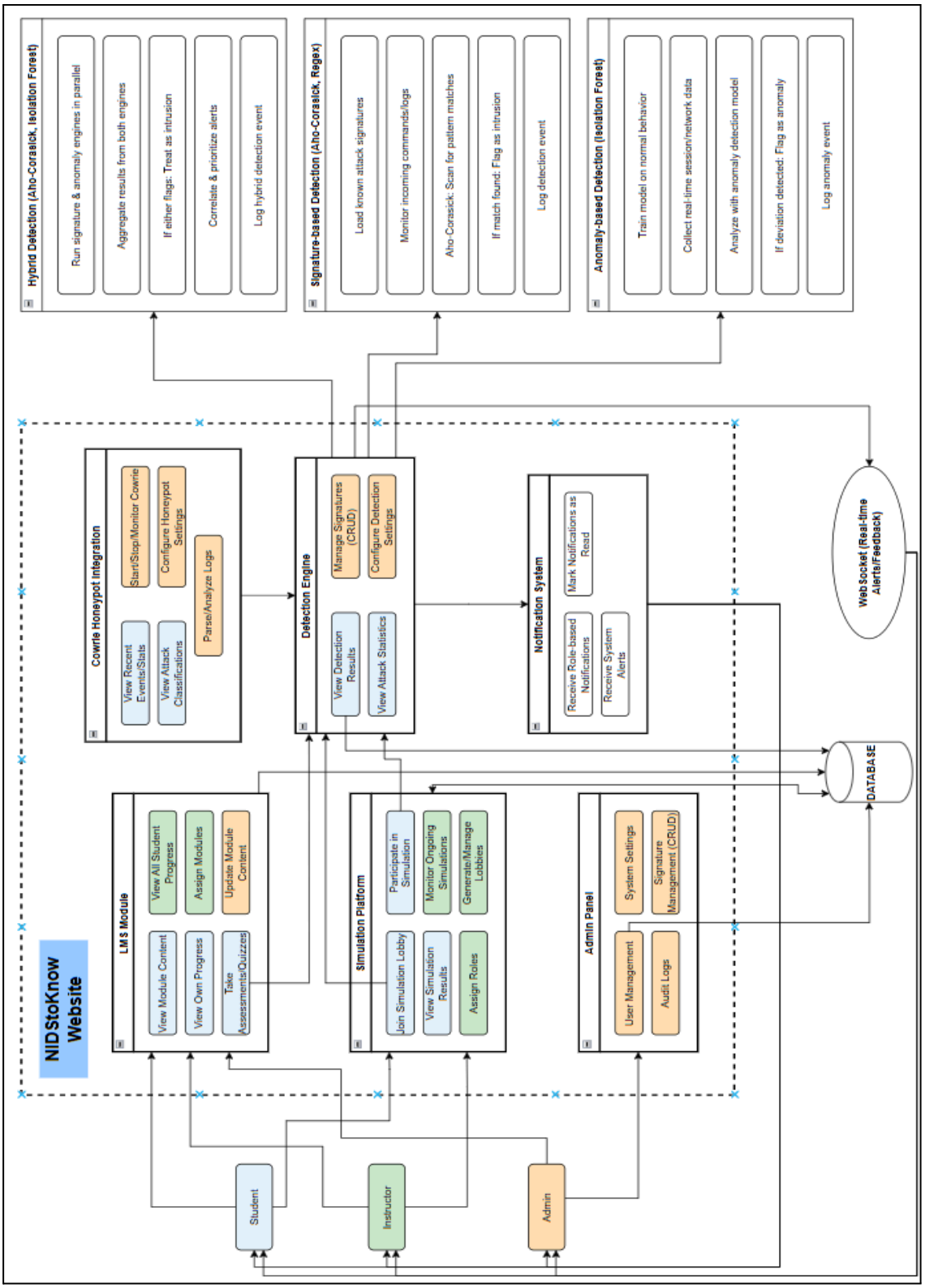

Figure 1. *Conceptual Framework of the System*

Project Purpose

The purpose of the NIDStoKnow is to create an effective platform for students to gain knowledge and simulate real-world scenarios utilizing the Cowrie Honeypot. Specifically, the project is dedicated to address lack of practical activities in IT courses in HEIs through the development of the simulation and learning platform.

The beneficiaries of the NIDStoKNow project encompasses a broad spectrum of stakeholders, each deriving distinct benefits:

IT Students. As the primary users, IT students are often limited to theoretical instruction with minimal exposure to real-world application. NIDStoKnow simulation environment may allow them to better understand various types of network intrusions and defensive strategies through hands-on activities.

IT Faculty and Instructors. As facilitators of learning particularly in HEIs, IT faculty and instructors often face challenges in providing practical cybersecurity experiences due to limited tools and resources. The NIDStoKnow platform may support their teaching by offering an accessible, interactive simulation environment that complements theoretical lessons with hands-on application.

Future Researchers. Future researchers require practical platforms to explore, validate, and extend cybersecurity models and techniques, particularly in the areas of NIDS and honeypot systems. NIDStoKnow may serve as a customizable and research-friendly environment for conducting experiments, gathering data, and analyzing attack behaviors in a controlled setting.

Scope and Limitation of the Study

This study focuses on the design, development, and implementation of NIDStoKnow. The platform aims to deliver both theoretical and practical activities

covering the three core NIDS methods: signature-based, anomaly-based, and hybrid. It will simulate attack scenarios using Cowrie focused on SSH and Telnet protocols to detect and examine malicious activities through a built-in Linux terminal in the platform. Interactive learning modules will be included to cover NIDS concepts and methods with assessments to measure the understandings in each lesson. Role-Based Access Control (RBAC) will be implemented to manage feature access for learners, instructors, and proponents as administrators. The system will also include tools for instructors to assign learning modules, monitor student engagement, and provide individualized feedback. The effectiveness of the platform will be evaluated through pre-tests and post-tests, with testing conducted in one of the HEIs located in Laguna.

The web-based platform for learning and real-world simulation in HEIs specifically designed for IT students, presents specific limitations: other forms of attacks such as those using Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Distributed Denial of Service (DDoS), systems cover different intrusion detection system such as Host-Based (HIDS), Cloud-Based (CIDS), and Distributed IDS (DIDS) are outside of its scope. The platform provides structured, built-in learning modules and simulations to support consistency across classes, although these are not designed for instructor customization. Additionally, the system is designed for desktop or laptop use only and needs an internet connection, posing challenges for users without reliable internet access. Lastly, the system evaluates learning effectiveness using pre-tests and post-tests only, which may not fully measure long-term understanding or real-world skill application.

CHAPTER II

REVIEW OF RELATED LITERATURE

Studies and Literature

Cybersecurity Education in HEIs

Cybersecurity education has become a strategic priority in higher education institutions as they increasingly face threats from cyberattacks that target sensitive academic and research data. Martini and Choo (2014) noted that traditional teaching approaches relying on passive methods, such as lectures and outdated content, often fail to prepare students for fast-changing realities in cybersecurity. Trickel et al. (2017) reinforced this by pointing out that many programs do not adequately simulate adversarial conditions, leaving graduates underprepared. Similarly, Kumar et al. (2013) identified gaps between classroom instruction and the practical skills required in real-world settings. In the Philippines, Oducado et al. (2022) found that students, even outside IT disciplines, exhibited limited awareness and poor practices in cybersecurity, while Buenaventura et al. (2024) reported age-related trends in cybersecurity awareness, revealing broader challenges in integrating effective digital security education across higher education.

Efforts to address these shortcomings emphasize the importance of adopting frameworks and programs that strengthen both institutional resilience and student preparedness. Bondoc and Malawit (2020) argued that Philippine higher education institutions must adopt regulatory measures to guide universities toward stronger protection mechanisms. Yuhong, Zhuo, and Monreal (2024) designed a network security architecture for smart campuses in the Philippines, highlighting the

importance of multi-layered security that integrates access control, authentication, and incident response. More recently, De Ramos and Esponilla (2025) examined several state universities in Metro Manila and concluded that structured, sustainable cybersecurity programs—aligned with international best practices—are necessary to address local institutional needs. Together, these perspectives show that strengthening cybersecurity education requires not only modernized curricula but also coordinated policy-level initiatives that reinforce both institutional and student capacity.

At the classroom level, interactive and experiential methods are proving effective in bridging the gap between theory and practice. Salazar et al. (2013) demonstrated how gamification strategies such as role-playing and simulations promote engagement and enhance decision-making skills in simulated cyber environments. Bond (2017) showed that competitive challenges encourage problem-solving under pressure, further enhancing learning outcomes. Al-Balushi and Martin-Hansen (2019) argued that pairing these approaches with applied training and research projects allows students to develop stronger conceptual understanding while also building practical competence. Bernhardsson et al. (2017) added that hands-on activities improve retention and adaptability, both of which are crucial for future cybersecurity professionals. For Philippine higher education institutions, integrating these methods can ensure that students acquire not only technical expertise but also the adaptive skills needed to respond effectively to complex and evolving cyber threats.

Learning Management System for Cybersecurity

Learning Management Systems (LMS) are extensively utilized in cybersecurity instruction to provide structured and accessible training. Ahmed (2024)

conducted a systematic review emphasizing how digital platforms integrate course materials with hands-on activities to strengthen learning. Similarly, Prümmer et al. (2024) examined cybersecurity training approaches, highlighting the effectiveness of combining LMSs with simulation-based environments to enhance skill development. Supporting this integration, the National Institute of Standards and Technology (NIST, 2023) introduced the Range Learning Management System (RLMS), which manages laboratories and assessments within cyber ranges. IBM (2024) further described cyber ranges as essential for creating authentic training environments, while Ukwandu et al. (2020) analyzed their use in education and testing. In addition, LMS platforms often provide instructor dashboards and analytics tools, enabling educators to monitor learner interactions, assess engagement, and deliver timely, personalized feedback, which has been shown to improve outcomes (Tirado-Olivares et al., 2024).

Complementing LMS features, learning modules play a vital role in structuring content and sustaining student engagement. Masaguni et al. (2023) demonstrated that project-based modules improved student participation and comprehension of complex subjects, while Croft (2018) emphasized the importance of fostering intrinsic motivation rather than relying solely on assessments. Az-Zahra et al. (2023) highlighted how well-designed modules encourage active participation through student-centered approaches. Similarly, Holmgren et al. (2019) found that modules promote reflection and adaptability in professional education. These findings collectively suggest that integrating structured modules into LMS platforms not only organizes content but also enhances learner motivation and understanding, aligning with modern pedagogical frameworks.

LMS platforms are not only designed to deliver instructional content but also to equip instructors with tools for assigning modules, monitoring engagement, and

delivering feedback. Hattie and Timperley (2007) emphasized that timely and specific feedback significantly enhances student learning, a principle many LMSs embed through rubric-based grading, annotation features, and structured return workflows. Engagement tracking tools such as dashboards and analytics further allow educators to monitor learner activity, identify at-risk students, and provide personalized interventions. Kaliisa et al. (2023) reported that dashboards increase student motivation and participation when instructors act on engagement data, while Tirado-Olivares et al. (2024) found that real-time monitoring features within LMSs improve the effectiveness of feedback and overall learning outcomes. Similarly, Lee et al. (2025) highlighted that the pedagogical integration of analytics by instructors is key to transforming monitoring data into actionable support for learners.

Simulation Platforms

Simulation platforms function as essential educational resources in cybersecurity training by providing immersive, practical experience in settings that replicate real-world systems and threats. Kebande (2024) assessed virtual laboratories (V Labs) for cybersecurity online education, discovering favorable views from educators and students regarding active learning, engagement, and problem-solving skills. Čeleda et al. (2020) presented KYPO4INDUSTRY, a platform aimed at simulating industrial control systems through adaptable modules, allowing students to develop educational games that mirror authentic cyberattack situations. In a similar vein, Švábenský et al. (2018) detailed how undergraduate students improved their adversarial thinking by creating serious games in a cyber range environment, with peer assessments validating the educational significance of their projects.

Oikonomou et al. (2021) suggested creating multi-domain cyber ranges, like interconnected European and maritime ranges, attaining real-world accuracy via the modular integration of physical and virtual systems. Topham et al. (2016) examined various kinds of cybersecurity labs (physical, simulation, virtual) and highlighted the significance of adaptability, managerial oversight, and scalability in effective simulation settings. Beuran et al. (2018) developed CyTrONE, a unified cybersecurity training framework that merges attack-, analysis-, and defense-focused tasks, featuring intuitive interfaces and adaptable environment management to simplify operational complexity and enhance overall educational processes.

Network Intrusion Detection System

Building NIDS is very important for keeping networks safe in different organizations. NIDS consists of three methods which are signature-based, anomaly-based, and hybrid detection. Signature-based looks for unknown patterns like or “signatures” in network traffic. Anomaly-based watches for anything unusual compared to normal behavior. The hybrid method combines both signature-based and anomaly-based methods to be more accurate. These systems usually have three main parts: sensors to watch the network traffic, servers to analyze the data, and consoles to manage everything (Sayed & Taha, 2023). Thanks to new technology like artificial intelligence (AI) and machine learning (ML), NIDS are now much better at finding threats. For example, ML methods such as decision trees, naïve Bayes, and support vector machines help the system learn from past data and spot attacks in the future (Jain & Waoo, 2023). These tools make it easier for NIDS to detect both common and new types of cyberattacks while making fewer mistakes (Vanin et al., 2022).

Even with these improvements, using NIDS can still be hard because hackers

are always coming up with new tricks. Old methods that look for specific, known attack patterns (called signature-based detection) do not work well against brand-new attacks (Banik & Peña, 2015). Because of this, experts are now focusing on finding unusual behavior in the network, which might show a threat even if it has not been seen before (Sivanantham et al., 2023). Some systems also use data mining to find hidden patterns that could mean someone is trying to break in (Sivanantham et al., 2023). Newer approaches like deep learning, especially with convolutional neural networks, and smart ways of picking which data to focus on, help make these systems more accurate and quicker to react (Qi et al., 2019; Ho et al., 2021).

Cowrie Honeypot

Cowrie is a medium-interaction honeypot designed to capture malicious behavior, offering insights into how attackers operate without compromising real systems. By emulating vulnerable SSH and Telnet services, it deceives intruders into revealing their methods, which are then recorded for analysis. Morić et al. (2024) highlight its growing use in both professional and academic environments, where it helps analyze intrusion techniques and supports hands-on cybersecurity training. Data collected from Cowrie can improve machine learning models used in intrusion detection, allowing these systems to identify and respond to threats more effectively (Tinnaluri & Shaik, 2024).

In addition, Cowrie's open-source nature encourages ongoing development and integration with threat intelligence platforms. According to Naik et al. (2020), the honeypot has successfully captured a variety of attacks, from brute-force logins to the deployment of malicious scripts. This adaptability makes Cowrie an invaluable tool for real-time threat detection and analysis, as it continuously evolves with emerging

attack methods. Studies have also shown that the data collected by Cowrie, when analyzed, can provide key insights into attacker behavior and techniques, which can then be used to improve cybersecurity models and predict future threats (Mispriatin et al., 2022). Furthermore, Cowrie's integration with other security systems, such as Intrusion Prevention Systems (IPS), allows for a more proactive defense mechanism, where the system can not only capture attacks but also mitigate them in real-time (Susanti et al., 2022).

Aho-Corasick Algorithm

The Aho-Corasick Algorithm, developed by Alfred V. Aho and Margaret J. Corasick (1975), is widely regarded for its efficiency in multi-pattern string matching. It operates through a finite automaton that processes all input patterns simultaneously, achieving a linear time complexity relative to the input size and total pattern length. This makes it particularly suitable for applications that involve scanning for multiple keywords or signatures, such as intrusion detection systems, antivirus scanning, and text processing (Stephen, 1994; Aho & Corasick, 1975). In educational applications, ACA has been employed to analyze the validity of examination items, where it tokenizes and evaluates test content against predefined rules (Omictin et al., 2023). The finite state nature of ACA allows systems like Quiz-Zone to quickly determine the presence of undesired constructs, e.g., "all of the above" options in multiple-choice tests which violate test validity guidelines (Omictin et al., 2023; Knipp, 2006). This demonstrates ACA's practical utility not only in technical domains but also in educational assessment technologies.

Nonetheless, ACA faces limitations when applied to scenarios demanding nuanced contextual understanding. For example, in Omictin et al. 's (2023)

implementation, ACA could not fully validate certain test formats, such as matching-type questions requiring semantic comparison of column lengths or short-answer items needing precise blank placement. In such cases, ACA's deterministic finite automata fall short due to their inability to evaluate relative lengths or understand conceptual alignment (Omictin et al., 2023). To address these shortcomings, Liangxu and Linlin (2012) proposed enhancements to ACA's memory efficiency through improved automaton storage formats, such as sparse-row and banded-row structures, which reduce overhead without compromising pattern matching accuracy. Their work suggests that with memory and performance optimizations, ACA could be extended to more memory-sensitive domains like embedded systems and real-time analytics (Liangxu & Linlin, 2012). These adaptations reveal the ongoing relevance of the Aho-Corasick framework, especially when combined with complementary algorithms or domain-specific rule sets to overcome its core limitations.

Isolation Forest Algorithm

Liu et al. (2008) introduced the Isolation Forest (iForest) algorithm as a novel and efficient anomaly detection method that isolates anomalies instead of profiling normal data. Unlike traditional methods such as statistical modeling, classification-based, and clustering-based techniques (Jain et al., 1999; Bishop, 1995; Rousseeuw & Leroy, 1987), iForest focuses on recursively partitioning data points, with the idea that anomalies are more susceptible to isolation and thus appear in shorter paths within tree structures. This method avoids the computational costs of distance or density calculations (Breunig et al., 2000; Knorr & Ng, 1998), allowing iForest to scale linearly in time and memory. The algorithm also performs well in

high-dimensional settings and with large datasets, effectively minimizing swamping and masking effects through sub-sampling.

Chua et al. (2024) applied the iForest model to a real-world context, detecting anomalies in web traffic using server log data from an e-commerce website. The study implemented a full machine learning pipeline, including data cleaning, transformation, and feature engineering, to prepare the dataset for anomaly detection. They referenced Tan et al. (2002) in emphasizing the importance of scalable anomaly detection for intrusion systems and incorporated derived features such as URI length and IOC occurrences alongside one-hot encoding and normalization. Their approach yielded high precision and recall rates. Furthermore, they cited Priyanto et al. (2021), Zhang et al. (2022), and Chabchoub et al. (2022), who examined improvements and evaluations of Isolation Forest in related anomaly detection settings, supporting its adaptability in modern cybersecurity applications.

Role-Based Access Control

Role-Based Access Control is a commonly used framework for managing access rights by allocating permissions to organizational roles instead of to individual users. Initially formalized by Ferraiolo, Gilbert, and Lynch (1995), RBAC has evolved into a cornerstone of enterprise security frameworks. Sandhu and Samarati (1994) pointed out its scalability in extensive organizations, whereas Hu et al. (2015) underscored its conformity with the principle of least privilege. According to Chen and Crampton (2012), role engineering is crucial to avoid permission creep, while Ni, Bertino, and Lobo (2007) suggested administrative frameworks that assist in delegation and policy enforcement. Crampton and Khambhammettu (2008) explored RBAC delegation, highlighting its significance in maintaining separation of duties and meeting regulatory compliance. Hu and Kuhn (2018) also connected RBAC to

accountability and auditability by means of organized access assignments, emphasizing its importance in enterprise governance.

RBAC has developed over time to meet contemporary challenges in cloud, IoT, and hybrid settings. Kuhn, Coyne, and Weil (2010) presented attribute-enhanced RBAC, integrating it with attribute-based access control (ABAC) to enable more context-sensitive choices. Xu, Zhang, and Wang (2020) introduced hybrid RBAC-ABAC frameworks designed for intricate enterprise applications, whereas Zhao and Bai (2018) examined dynamic RBAC for cloud settings, highlighting adaptability in multi-tenant architectures. Dlamini and Eloff (2019) examined RBAC in IoT, highlighting challenges in implementing it on resource-limited devices. Alotaibi and Alsubaie (2021) researched RBAC in higher education, demonstrating its efficiency in safeguarding sensitive academic and research information. Together, these investigations validate RBAC's flexibility in changing digital environments while preserving its fundamental benefits of scalability, accountability, and compliance

Related System

The table 1 compares the distinct strengths of NIDStoKnow against four related systems such as App 1, App 2, App 3, and App 4 across ten essential features relevant to cybersecurity learning and network intrusion detection.

NIDStoKnow is uniquely designed as a fully web-based platform, allowing users to access it directly through a browser without any local installation. This greatly improves accessibility and convenience, especially for educational institutions. In contrast, App 1, App 2, and App 4 require local installation, limiting their scalability in classroom or remote learning environments. App 3, on the other hand, is

generally web-based but varies across vendors, so while many offer web access, this is not uniform. Similarly, NIDStoKnow's core purpose is educational, providing a guided, interactive environment for IT and cybersecurity students to learn hands-on. By comparison, App 1 and App 2 are primarily professional-grade security tools used in operational networks, lacking dedicated educational features. App 3 often blends education and professional training, but their focus and content vary depending on the provider, whereas App 4 is mainly a commercial honeypot tool without a learning-oriented design.

Moreover, NIDStoKnow incorporates the Cowrie honeypot to capture real attacker behavior for practical learning. In contrast, App 4 also uses honeypots but is targeted toward enterprise security rather than education. The use of honeypots in App 3 varies significantly by vendor and platform capabilities; some include honeypots as part of their training simulations, while others do not. App 1 and App 2 do not use honeypots at all.

Moving on to detection methods, App 1 is well-known for its robust signature-based intrusion detection capabilities. App 2 and most App 3 platforms also support signature detection, though App 3's features vary widely by vendor. App 4 does not focus on signature detection, relying instead on honeypot technology. NIDStoKnow supports signature-based detection as part of a comprehensive learning experience. When it comes to anomaly detection, App 2 supports this by identifying unusual traffic patterns. App 3 varies here, as some vendors provide anomaly detection while others do not, hence the "depends" rating. NIDStoKnow includes anomaly detection to teach multiple detection techniques, while App 1 and App 4 focus primarily on signature-based or honeypot methods and lack strong anomaly detection. Hybrid detection, which combines signature and anomaly methods for

better accuracy, is offered by both App 2 and NIDStoKnow to provide advanced learning and operational capabilities. However, App 3 again varies widely; some vendors offer hybrid detection, others do not, so it is marked “depends.” App 1 and App 4 do not support hybrid methods.

Furthermore, NIDStoKnow stands out with a built-in attack simulation module that lets students practice detecting threats in a safe, controlled setting. App 3 platforms generally offer attack simulations, but their scope and quality vary by vendor and platform. App 1, App 2, and App 4 do not provide simulation features, focusing solely on detection. In terms of visualization, NIDStoKnow offers rich dashboards that present logs and alerts in an intuitive way to help learners understand complex data. App 2 also provides advanced visualization tools for professional monitoring. Visualization capabilities in App 3 vary widely across vendors, from minimal to comprehensive. App 1’s visualization is limited because it mainly operates as a detection engine, relying on external tools for visualization, while App 4 provides only basic visualization aimed at enterprise use. Additionally, only NIDStoKnow features an embedded Linux terminal directly within its web interface, enabling users to analyze logs and execute commands without external terminal software. The other systems require users to access external or third-party terminals, which adds complexity, especially in an educational context. Lastly, NIDStoKnow is intended to be open-source or free for academic use, enhancing accessibility. App 1 and App 2 are open-source and free, widely used by professionals and educators. App 3 platforms are mostly commercial products with proprietary licenses, making them less accessible, while App 4 is fully commercial, requiring purchase and licenses.

Table 1. Systems Comparison

	APP 1	APP 2	APP 3	APP 4	NIDStoKNOW

1. Web-based platform	X	X	✓	X	✓
2. Educational Focus	X	X	✓	X	✓
3. Uses honeypot	X	X	✓ (varies)	✓	✓
4. Supports signature-based detection	✓	✓	✓	X	✓
5. Supports anomaly-based detection	X	✓	✓	X	✓
6. Supports hybrid-based detection	X	✓	Depends	X	✓
7. Simulation attacks for learning	X	X	✓	X	✓
8. Comprehensive visualization tools	Limited	✓	Varies	Limited	✓
9. Linux Terminal (embedded)	X	X	X	X	✓
10. Open-source/free	✓	✓	Mostly commercial	Commercial	✓ (academic)

Synthesis

In the ever-changing world of cybersecurity, increasing cyber threat complexity has made conventional security protocols inadequate, especially within educational settings where awareness and readiness are paramount. As highlighted by Azizan et al. (2021) and Ibraheem (2022), advanced machine learning and deep learning methodologies have made contemporary NIDS more robust, yet such advancements are frequently underutilized within HEIs because of restricted access to interactive and real-world-oriented learning resources. Conventional cybersecurity education in HEIs, as explained by Xiao et al. (2023) and Martini & Choo (2014), is

plagued by out-of-date curricula and passive pedagogy that does not equip students to cope with the reality of advanced threats.

Evidence indicates that the integration of theoretical and practical strategies greatly improves the level of learning (Al-Balushi & Martin-Hansen, 2019; Vauderwange et al., 2019). Nonetheless, there still lacks a specialized platform that can efficiently mimic network attacks and expose students to hands-on experience in intrusion analysis. While LMS provide skeletal support in the distribution of teaching material (Anderson, 2008; Fritz, 2016), they are typically not deployed with in-built tools for cybersecurity simulation, attack visualization, or live terminal interaction.

To fill this void, compared related systems like the App 1, App 2, App 3, and App 4 provide some NIDS features but lack in providing a web-based, pedagogy-oriented, and integrated learning environment. App 1 and App 2 are strong but are not pedagogically oriented; they do not have simulation tools and inculcated educational infrastructure. App 3 are closer in training scenario but tend to be resource hungry, expensive, and lack open-source flexibility. App 4, as a Windows-based honeypot deployment tool, falls short for hybrid NIDS model support and doesn't focus on interactive student learning.

NIDStoKnow fills this gap in a unique place. With the integration of Cowrie honeypot to simulate signature-based, anomaly-based, and hybrid detection mechanisms in a web-based learning platform, it offers comprehensive and experiential training in an immersive and accessible environment particularly designed for students of IT. The integration of a Linux terminal within the training environment, complete visualization tools, and attack simulation allows learners to experience real-world attacks within a sandboxed yet meaningful environment, filling the void between theoretical education and practical cybersecurity application.

Furthermore, its open-source nature encourages institutional adoption without financial barriers.

CHAPTER III

METHODOLOGY

Research Design

The research design incorporates both descriptive and developmental approaches. The combination of descriptive and developmental research design enables a comprehensive understanding of the NIDS methods through theoretical and practical tasks. Developmental research facilitates the creation of an effective educational and simulation platform, while descriptive research gives knowledge base. The NIDStoKNow project intends to obtain insights into the inadequacy, create a strong solution, and continuously enhance the system based on user's feedback and evaluation by combined research designs.

According to Creswell (2017), descriptive research is used to observe and describe situations, populations, or phenomena, with the goal of collecting data to identify patterns and trends. In this study, the focus is on exploring and recording IT students' understanding of NIDS, their learning challenges, and their preferred methods of learning through interviews, literature reviews, as well as pre- and post-test assessments.

The developmental phase involves the design and creation of a web-based platform for learning and real-world simulation of NIDS using the Cowrie Honeypot. Developmental research, as defined by Richey and Klein (2014), involves an iterative process of design, implementation, and user feedback, aimed at improving instructional programs and materials. This iterative approach helps the system effectively address identified challenges and enhances understanding of NIDS through practical, real-world scenarios.

Population of the Study

The population of this study is composed of eight (8) IT experts who are graduates of IT-related programs and are currently working in the industry. They were chosen for their professional experience and technical expertise, which are essential in evaluating systems related to cybersecurity and software development. Their background enables them to provide credible and relevant assessments of the proposed platform.

These experts are expected to evaluate the system based on the ISO/IEC 25010 software quality model, which covers the characteristics of functional suitability, reliability, performance efficiency, usability, security, compatibility, maintainability, and portability. By drawing from their industry knowledge and applied skills, the participants can deliver informed feedback that ensures the platform meets both technical standards and practical requirements in real-world use.

Sampling Design

This study employed a purposive sampling technique, a non-probability method in which participants are intentionally selected based on specific qualifications relevant to the research. The respondents were chosen for their academic background in IT-related programs, current employment in the IT industry, and professional experience in areas such as system development, cybersecurity, and software evaluation.

Purposive sampling was deemed appropriate because the study required expert judgment to evaluate the proposed platform. This technique is commonly used in studies where specific expertise is necessary, as it allows researchers to deliberately

select individuals who can provide the most relevant and reliable information (Etikan, Musa, & Alkassim, 2016). By involving participants with the required knowledge and practical expertise, the research ensured that the evaluation results were credible, reliable, and aligned with the technical requirements of the study.

Data Collection Instrument

The researchers utilized both primary and secondary sources of data to obtain thorough and dependable information.

Interviews. The researchers conducted structured interviews with selected third and fourth year BSIT students majoring in Network Administration to evaluate their understanding of NIDS. Most third year students acknowledged having limited knowledge about NIDS and its methods: signature based, anomaly based, and hybrid, and suggested the need for dedicated learning tools and practical activities. Fourth year students showed slightly better awareness, with some having encountered tools like Snort, but their understanding remained uneven due to limited academic coverage. Therefore, both groups emphasized the importance of incorporating more focused and hands-on instruction on NIDS within the curriculum to strengthen their knowledge and skills in cybersecurity.

Documentary Analysis. The researchers collected secondary data through comprehensive online searches, aiming to understand and position their study within the framework of existing knowledge. The chapter opens with a review of related literature, examining established theories, concepts, and insights on NIDS and possible integrations that can address the absence of practical, hands-on learning environments. Through the review of academic articles, research studies, and existing systems, the researchers obtained valuable insights into NIDS and current approaches

to bridging gaps in cybersecurity education. They evaluated relevant literature for practical applications and overall effectiveness. This analysis revealed common patterns and unmet needs, forming the basis for the study's framework, data gathering, and analytical methods.

Evaluation Form. To evaluate the overall quality of the proposed system, the researchers employed a researcher-made questionnaire based on the ISO/IEC 25010 software quality model. This international standard provides a structured framework for assessing software products using eight quality characteristics: functional suitability, reliability, performance efficiency, usability, security, compatibility, maintainability, and portability. The instrument utilized a 5-point Likert scale ranging from 1 – Strongly Disagree to 5 – Strongly Agree to measure expert evaluators' perceptions of the system's performance against these characteristics. This tool ensured that NIDStoKnow was assessed comprehensively, both technical and functional aspects of the platform, following global software evaluation practices.

Statistical Treatment

The study employed descriptive statistics, with a focus on the average to analyze and summarize the evaluation data. This measure enabled the researchers to determine the central tendency and observe how the data values were distributed. Table 2 presents the average as a key metric to identify important characteristics and trends within the data, providing a clear understanding of the overall results. The average was calculated by summing all response values and dividing by the total number of responses, allowing for systematic analysis of the Likert scale ratings.

Table 2. Statistical Treatment for Evaluation Form

ANALYSIS	STATISTICAL TOOLS
8 IT experts' evaluation based on ISO/IEC 25010 Software Quality Model	Average

Formula for calculating the average:

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

This equation represents the formula for computing the average, also called the arithmetic mean, of a set of numbers. The researchers applied this formula to find the central value of the dataset by adding all individual numbers together and dividing the total by the number of values.

Average = (Sum of all numbers) / Number of numbers

Where:

- $\overline{X}$ = average (arithmetic mean)
- X_i = each individual number in the set
- n = total number of numbers in the set
- $\sum$ = summation

Table 3 presents the numerical values that each category of the Likert scale represents, where Frequency is the frequency that each category has been selected by the respondent. It is this strategy that enables us to convert ordinal Likert scaling data to number allowing a concise interpretation of the opinion that the respondents provided. This focused application of the average as the singular measure of central tendency aims to capture the central position of the data straightforwardly and comprehensively, facilitating a clear and concise analysis.

Table 3. Likert Scale for ISO/IEC 25010 - Software Quality

SCALE	NUMBER RATING	DESCRIPTIVE RATING
5	4.20 – 5.00	Strongly Agree
4	3.40 – 4.19	Agree
3	2.60 – 3.39	Neither Agree nor Disagree
2	1.80 – 2.59	Disagree
1	1.00 – 1.79	Strongly Disagree

Project Design

The proponents implemented the Agile Software Development Model for NIDStoKnow to guide the creation of the web-based platform. This approach emphasizes flexibility, collaboration, and continuous improvement, allowing the development team to adapt swiftly to changing requirements and stakeholder feedback. By employing Agile, the proponents can iteratively develop and enhance NIDStoKnow, incorporating changes and adjusting features based on suggestions and comments from the IT learners and instructors.

Software Development Model

Figure 2 consists of Plan and Requirements, Design, Develop, Test, Review, and Launch. Most of the platforms use this model because it doesn't focus on prototypes. It can be presented once it is completed. Agile uses an incremental delivery, short-cycled iterative, adaptive and collaborative methodologies (Omonije, 2024).

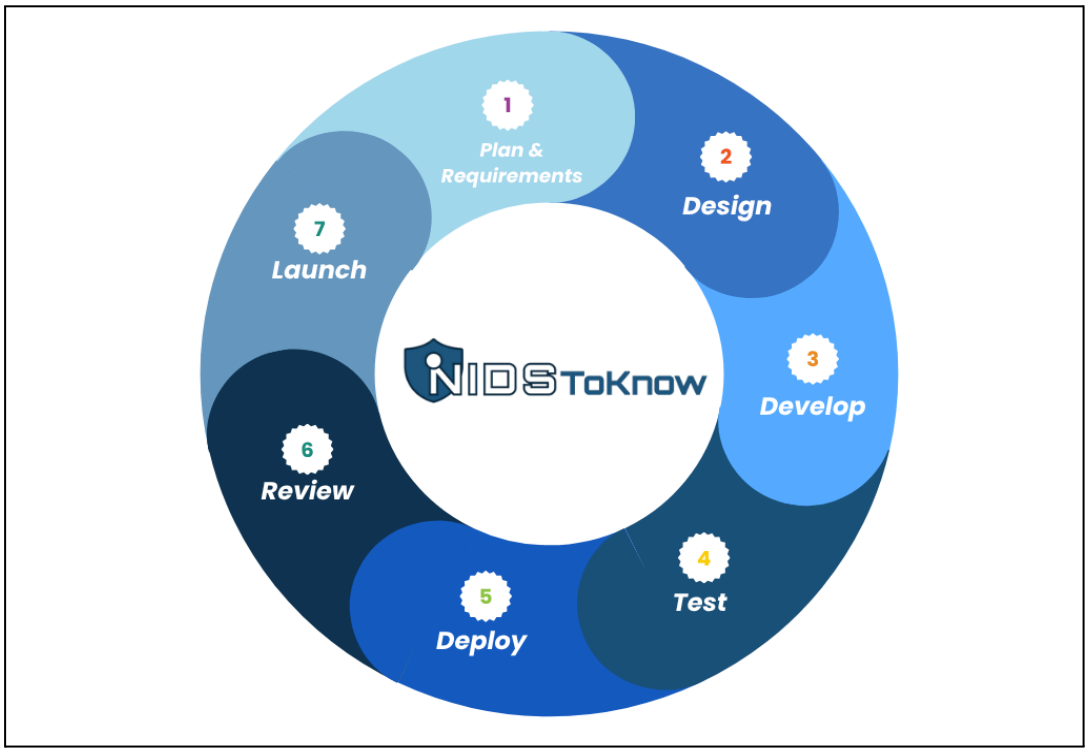

Figure 2. *The Stages of Agile Development*

Plan and Requirements

In the initial planning phase of the NIDStoKnow project, the researchers conducted interviews with third- and fourth-year Network Administration students shown in Figure 3 to identify the challenges they encountered in understanding NIDS, a key topic in their curriculum. These insights guided the formulation of system requirements and functionalities for a web-based learning platform. The project aimed to develop interactive simulations for signature-based, anomaly-based, and hybrid

detection methods to address the lack of hands-on learning experiences. Researchers defined user roles, consulted with a network security specialist, and conducted in-depth research to prioritize platform features, resulting in a detailed product backlog. Furthermore, the team estimated necessary resources, assigned roles, established a realistic timeline, and implemented strategies to manage scope creep, thereby ensuring a structured and goal-oriented planning process.

Figure 3. *Interview with 3rd Year and 4th Year NetAd Students*

For the documentation and development of the proposed system, the researchers required a range of essential tools and resources. These include a laptop or desktop computer, reliable internet connection, and various peripheral devices to facilitate their work. For the documentation and development of the proposed NIDStoKnow system, the researchers utilized a variety of essential tools and resources to enable a smooth and efficient workflow. Figure 4 presents the software applications intended for use throughout the design and development phases of the NIDStoKnow system. These include Canva for creating the project logo and visual assets, Figma for crafting the user interface (UI) and optimizing user experience (UX), and Visual Studio Code as the primary code editor for developing the web-based platform, which accommodates three user roles: admin, instructor, and

student. Additionally, the researchers employed Cursor AI, an AI-powered coding assistant, to enhance productivity by generating code snippets, debugging errors, and providing real-time coding suggestions. The strategic use of these tools allowed for a streamlined and collaborative workflow, integrating both visual design and backend functionality while supporting continuous testing and iterative improvement of the platform.

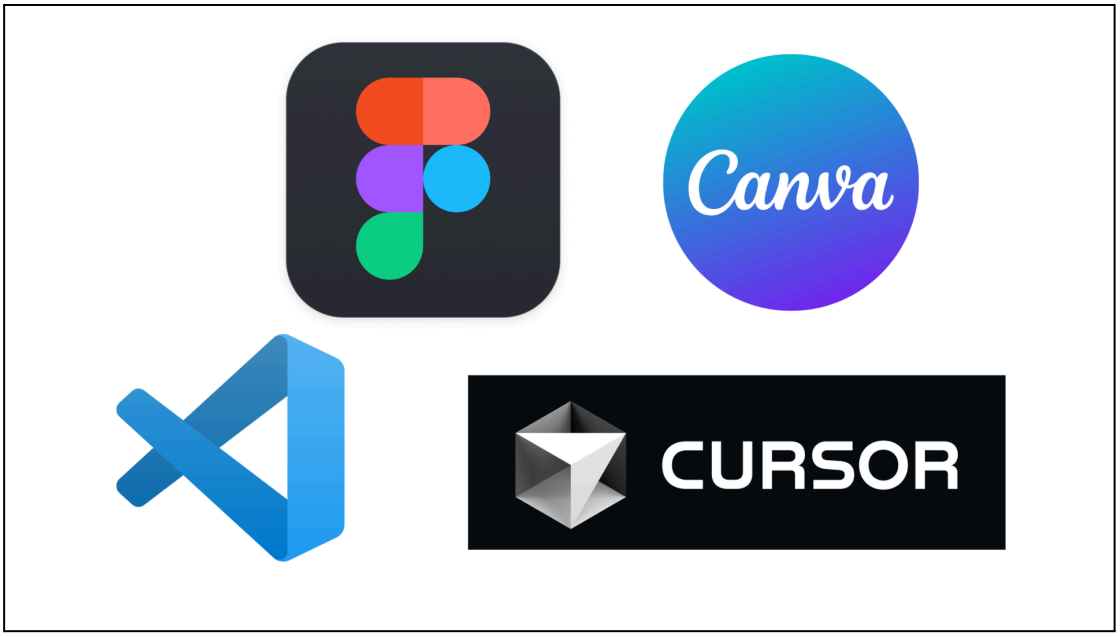

Figure 4. *Application Used in the Development of the System*

Design

After gathering data and requirements, the proponents proceed to design a user-centered interface that promotes the primary objective of the NIDSToKnow system. By identifying the users, they visualized the layout and flow that would align with the concept of a learning platform ensuring a minimal and visually appealing design for the users.

The design process involved multiple iterations, refining the layout, color schemes, and feature sets to optimize the system's functionality and effectiveness. Feedback from the adviser and panel members was considered to ensure the design is

aligned with the identified needs of the users. By prioritizing these needs, the system allows users to maximize usability and promotes effective learning experiences.

Figure 5 presents the logo and the theme of the system, which the proponents designed to convey the vibe of a learning platform imbued with elements of cybersecurity aligning with the project's objectives. The logo was conceptualized with a readable, tech-forward typography combined with a shield symbol to make it memorable. In terms of the color palette, the proponents explored a variety of colors to elevate the system's atmosphere, ultimately favoring navy blue. The visual appeal of the logo resonates with both the cybersecurity theme and the educational purpose of the system.

Similar to the system design and development, the logo underwent multiple iterations. With subtle refinements in typography weight and spacing, it was designed to maintain readability and balance on both dark and light backgrounds. The proponents paid careful attention to the logo's details to support user accessibility and usability. The creation of this logo would not have been possible without the help of modern tools like Canva and Figma.

Figure 5. *The Logo of NIDSToKnow System.*

Figure 6 presents the user interface of the system, designed to address the distinct needs of two user groups: students and instructors. For students, the interface provides structured learning modules, interactive simulations, and a lobby where they can assume various roles to perform specific tasks. This design promotes active, hands-on learning, allowing students to apply theoretical knowledge in simulated scenarios.

The instructor interface closely resembles the student interface with additional functionalities, such as monitoring student progress, managing content, and overseeing simulation activities. Incorporating feedback from advisers and evaluators, the user interface was carefully refined to ensure usability, functionality, and alignment with the system's educational objectives.

The integration of third-party services MySQL database was enhanced as the design process went along. Design changes were made to enhance database performance under increased loads to maintain its effective functionality in real-world settings after testing.

The Agile methodology made sure that the design phase was flexible and sensitive to user input and technological difficulties. By reviewing and modifying design decisions made at each sprint, the proponents were able to adapt to changing requirements, and solve problems related to the user interface, system architecture, or backend integrations. NIDSToKnow has developed into a complete, easy-to-use platform with a well-organized backend and a robust alerting system.

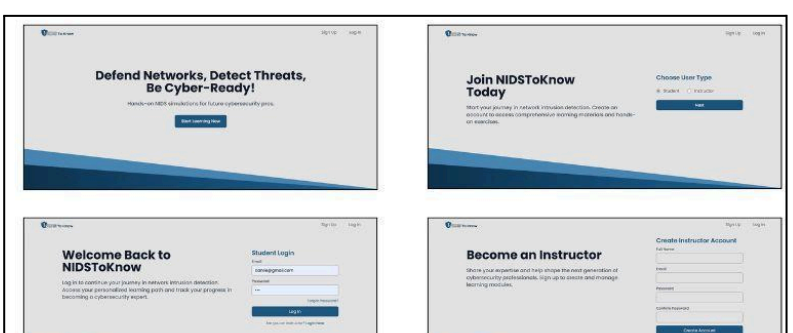

Figure 6. *User Interface of NIDSToKnow.*

Develop

During the NIDSToKnow development phase, the team adopted an Agile methodology, focusing on iterative and incremental implementation of the platform's core cybersecurity learning features.

The process was organized into short sprints with clear priorities set in the

product backlog. This approach enabled the team to deliver and test new features rapidly, ensuring that each component such as the Cowrie honeypot integration, interactive NIDS training modules, and the user dashboard was developed and refined in close collaboration with cybersecurity experts and educators.

The Figure 7 shows the technologies, languages, and libraries used throughout the development included Python, FastAPI, Uvicorn, Pydantic, MySQL Connector, WebSockets, python-jose, passlib, bcrypt, python-dotenv, aiofiles, python-dateutil, and pyahocorasick for the backend; JavaScript, React, Vite, Tailwind CSS, Material UI (MUI), Chart.js, Axios, and Xterm.js for the frontend; Cowrie honeypot for real-world attack data; MySQL for persistent storage; and WebSocket for real-time communication. Containerization was achieved using Docker for both backend and frontend deployment. Other technologies involved secure log management, signature-based detection using Aho-Corasick and regex, anomaly-based detection using the Isolation Forest machine learning algorithm, hybrid detection combining Aho-Corasick with Isolation Forest for enhanced accuracy, RESTful APIs, and real-time dashboards. The backend was implemented in Python using FastAPI, providing RESTful APIs for data processing, user management, and integration with the MySQL database. The Cowrie honeypot was integrated to collect real-world attack data, which was then processed and visualized for educational purposes.

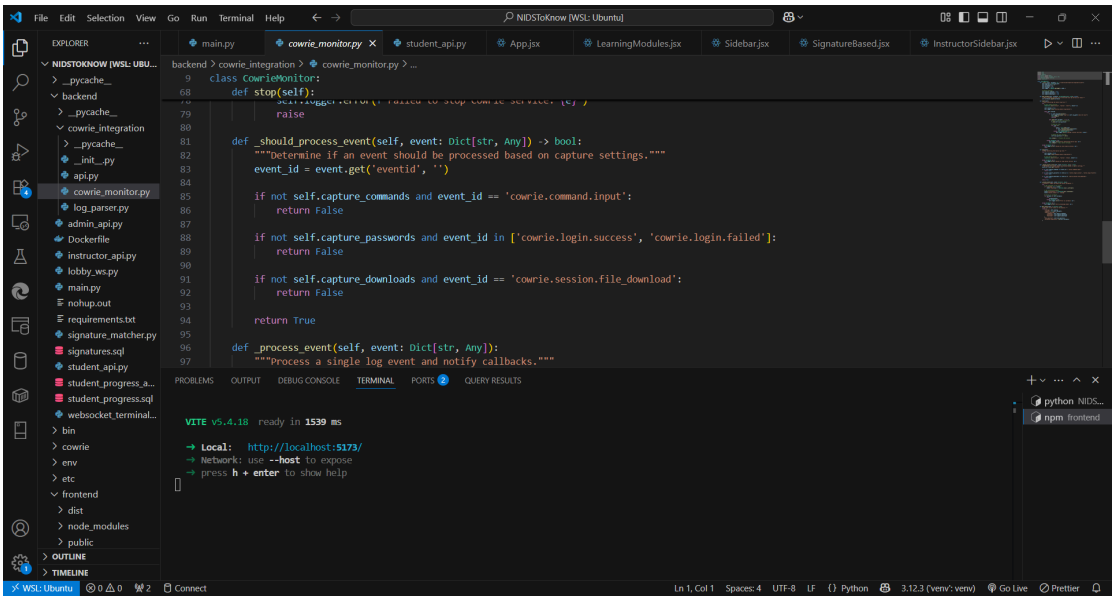

Figure 7. *Cowrie Honeypot Integration.*

Figure 8 illustrates the flow of Signature-based detection implementing the Aho-Corasick algorithm and regular expressions for efficient pattern matching, while anomaly-based detection was powered by the Isolation Forest algorithm to detect unusual behavior and unknown threats. The hybrid detection model utilized both Aho-Corasick and Isolation Forest, combining known pattern recognition with anomaly detection to provide a more comprehensive threat analysis.

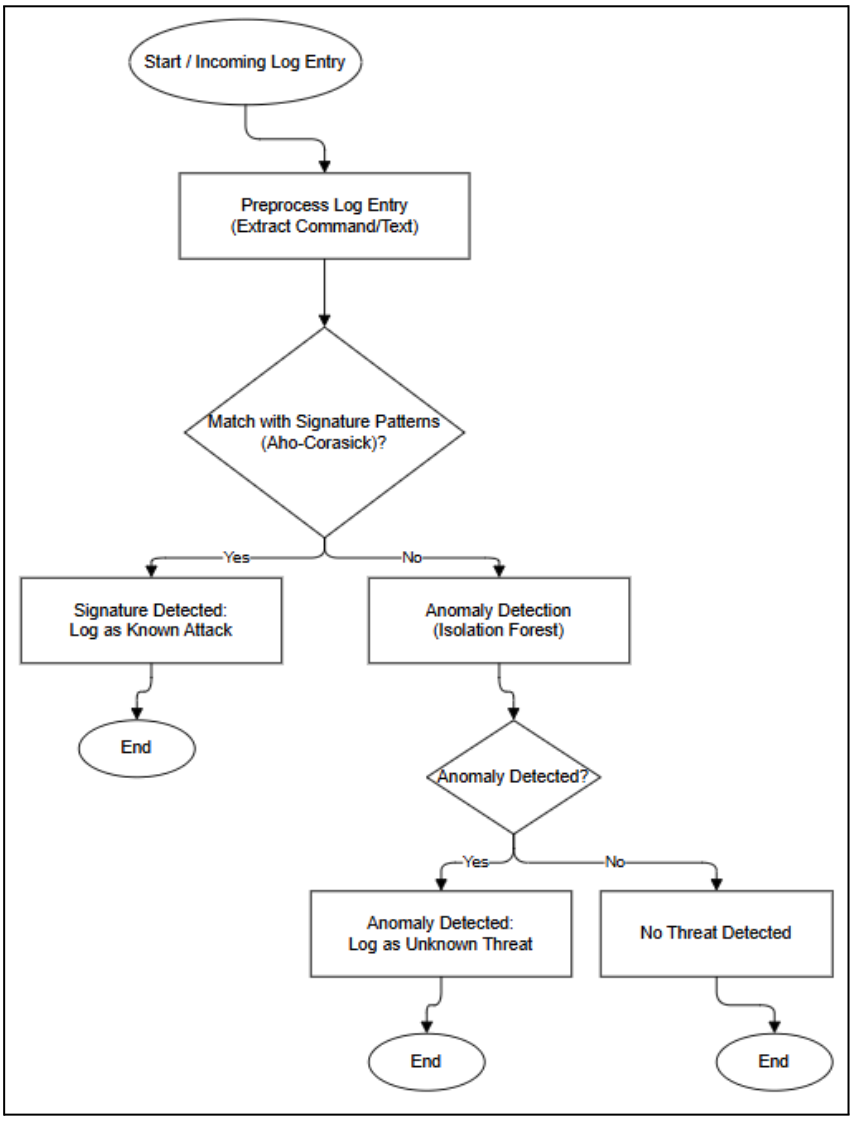

Figure 8. *Signature-Based and Anomaly Detection Flow.*

The figure 9 presents the frontend, proponents developed an intuitive dashboard using React, Vite, and Tailwind CSS, focusing on usability and a learning-friendly interface. Real-time data visualizations were incorporated using Chart.js to display threat analytics and student performance metrics, supporting hands-on learning and monitoring. Each sprint produced a working version of the dashboard, capable of pulling live data and presenting interactive training modules, quizzes, and educational content.

Throughout development, continuous integration and unit testing were employed to ensure that new code did not disrupt existing features. This practice maintained the platform's stability and security as new modules were added. The team also implemented secure log exporting and archiving, ensuring that sensitive data was handled appropriately.

By the end of the development phase, NIDSToKnow had evolved into a robust and comprehensive platform, supporting real-time NIDS learning with hands-on simulations, instructor tools, a user-friendly interface, and secure log management. Rigorous testing and verification ensured smooth operation in a production environment, aligning the product with the project's educational objectives and user needs.

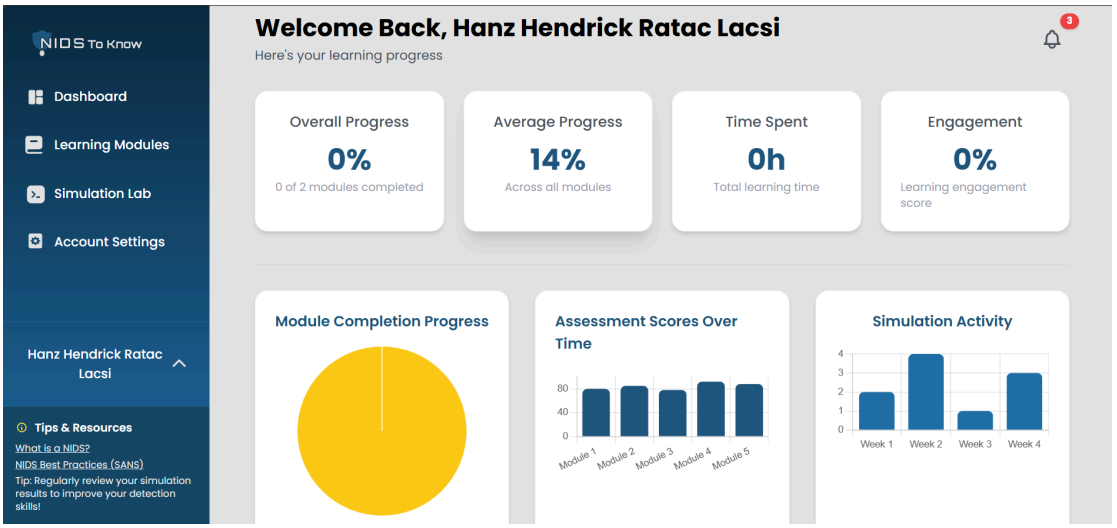

Figure 9. *NIDSToKnow Student Side Dashboard.*

Testing

This phase will focus on identifying and resolving system failures, such as bugs, functionality issues, and errors in NIDS simulations. Through structured testing activities, including theoretical modules, hands-on simulation of signature-based, anomaly-based, and hybrid methods, and honeypot-based attack detections. The

proponents will conduct debugging and system refinement to stabilize the core functionalities. This process directly supports the platform's objective to provide effective, interactive learning experiences while validating the proper integration of the Aho-Corasick and Isolation Forest algorithms.

Review

After initial testing, the review phase will involve the collection of feedback from selected IT experts through evaluation forms. This feedback will be analyzed to identify usability concerns, content clarity issues, and opportunities to improve system design, instructional value, and simulation effectiveness. Adjustments will then be made to enhance system performance and user experience particularly in areas like module delivery, threat visualization, and user interaction helping the platform remain aligned with its educational goals.

Launch

Once all feedback from the review phase has been addressed and final improvements have been implemented, NIDStoKnow will be officially launched for academic use under subscription-based access model. The platform will be fully functional, integrating all major features such as role-based access, simulated NIDS methods using Cowrie honeypot, algorithm-based detection modules, and instructor tools for monitoring engagement and performance.

Testing and Evaluation Procedure

CHAPTER IV

RESULTS AND DISCUSSION

This chapter presents the results of the study and discusses how these align with the methodology used in achieving the research objectives. The findings are presented based on the specific objectives, emphasizing the system's contribution to cybersecurity education. The discussion centers on how the platform supports both learning and teaching by combining theoretical instruction with practical application, while also demonstrating its usability and overall impact on students.

The researchers achieved the main objective of developing *NIDStoKnow*, a web-based learning and simulation platform for NIDS. Beyond serving as a tool for students, the system provides instructors with features for providing modules, monitoring learner engagement, and delivering feedback. It also integrates the Cowrie Honeypot to demonstrate real intrusion activities, allowing learners to observe network threats in practice. Figure 1 illustrates the Landing Page with the tagline, *"Defend Networks, Detect Threats, Be Cyber-Ready!"*, which welcomes users into the platform.

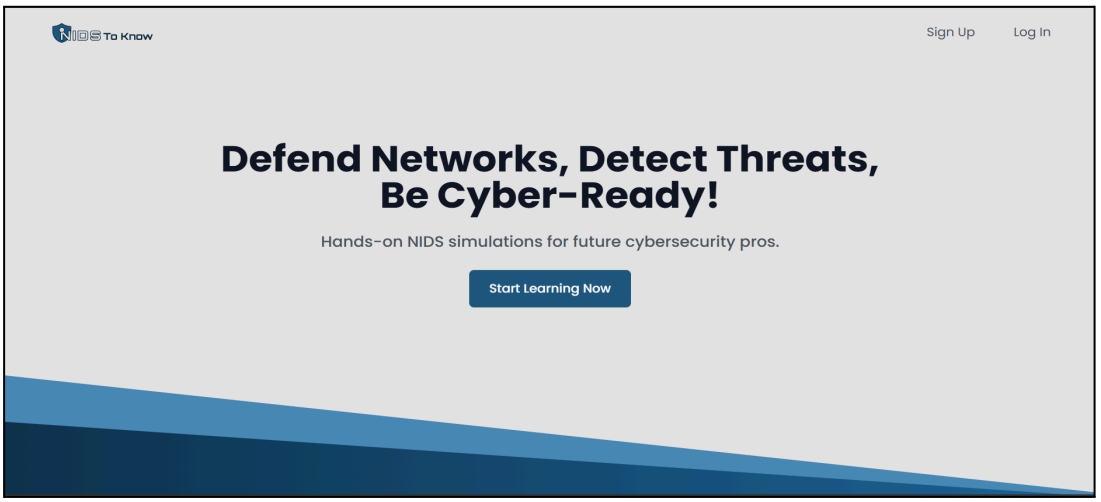

Figure 1. *NIDStoKnow Landing Page*

To design and develop a web-based learning and simulation platform

The proponents accomplished these specific objectives by developing a web-based platform designed for cybersecurity learning and simulation through the following features:

Theoretical activities focused on NIDS methods and interactive simulation to demonstrate detection approaches

Theoretical and interactive simulation activities were created focusing on NIDS methods and were integrated into the platform. As shown in Figure 1, the system's scope includes three learning modules that cover the fundamental concepts of NIDS: signature-based, anomaly-based, and hybrid intrusion detection. The theoretical component begins with basic topics and gradually progresses to advanced discussions. Each module provides an overview along with accessible buttons for Theory, Practical Exercise, and Assessment. The modules are organized by difficulty level: beginner, intermediate, and advanced— and indicate the estimated completion time. A status tracker also shows the learner's progress for each module. The problem addressed here is that traditional cybersecurity education often relies heavily on lectures and static resources, which limits students' ability to apply concepts in realistic scenarios (Alotaibi, 2022). With regard to this specific problem, the platform encompasses theories complemented with interactive exercises so that students learn the concepts and most importantly practice the steps of intrusion detection techniques within an offered simulation. This solution integrates the most recent theoretical and practical approaches to teaching and learning problem solving by the students. This approach correlates with the research stating that the combination of theory with practice improves studying and retention of the material over the time and skill sets

for the retention and the clinical practice in cybersecurity training.

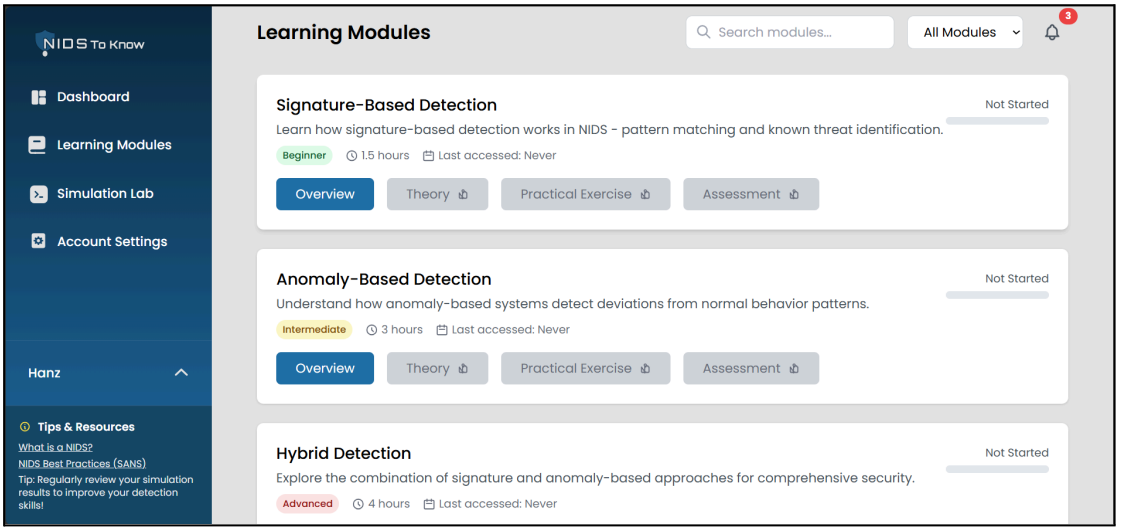

Figure 1. *Leaning Modules*

The proponents incorporated validated content as a systematic approach to the pervasive problem of e-learning materials infused with texts which likely decreases interest and retention (Mayer, 2021; Clark & Mayer, 2016). As depicted in Figure 1, each module has an assigned estimated time for completion and requires learners to complete an assessment before they can proceed; the assessment is critical and if it is not passed, the time is reset ensuring learners have complete mastery of the information before advancing to the next module. Within the modules, learners are provided a percentage of completion which enhances self-regulation as well as motivation. In one of the many studies performed by Abuhassna et al. (2020), it was discovered that modular e-learning systems which include time tracking, progress monitoring, and formative assessments significantly improve learner engagement and retention of information. The platform employs multimedia components such as images, videos, and interactive assessments related to the material so they can capture the learners attention, support understanding, and retention of the information through

active and passive learning by explaining the concepts through various lenses.

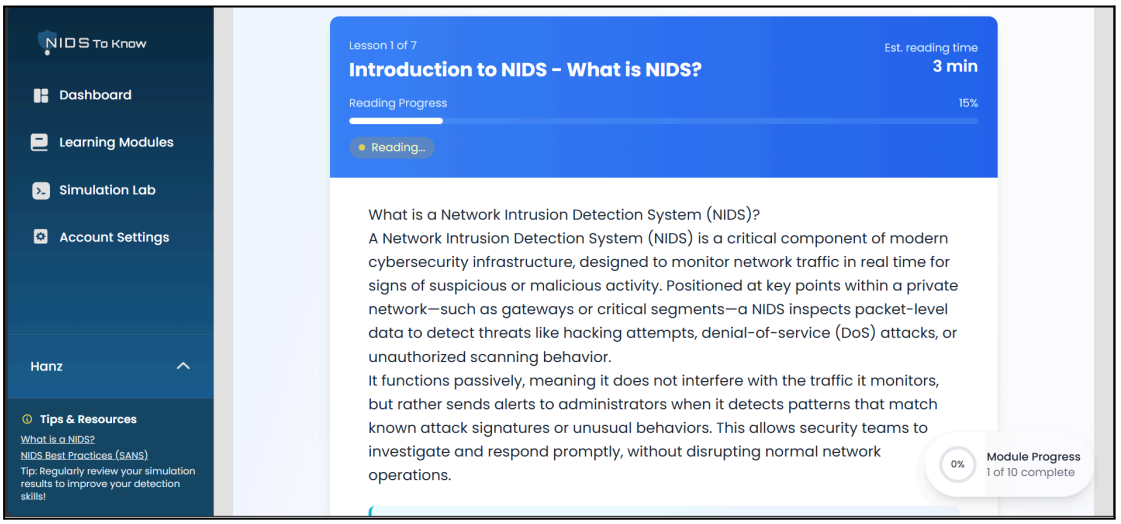

Figure 1. *NIDS Fundamentals Module*

Figure 1 presents the Signature-Based detection module, which introduces the method of identifying intrusions by matching network activity against a database of known attack patterns. It provides learners with clear explanations, essential terms, and illustrative examples to build a solid understanding of how signature-based detection works in NIDS.

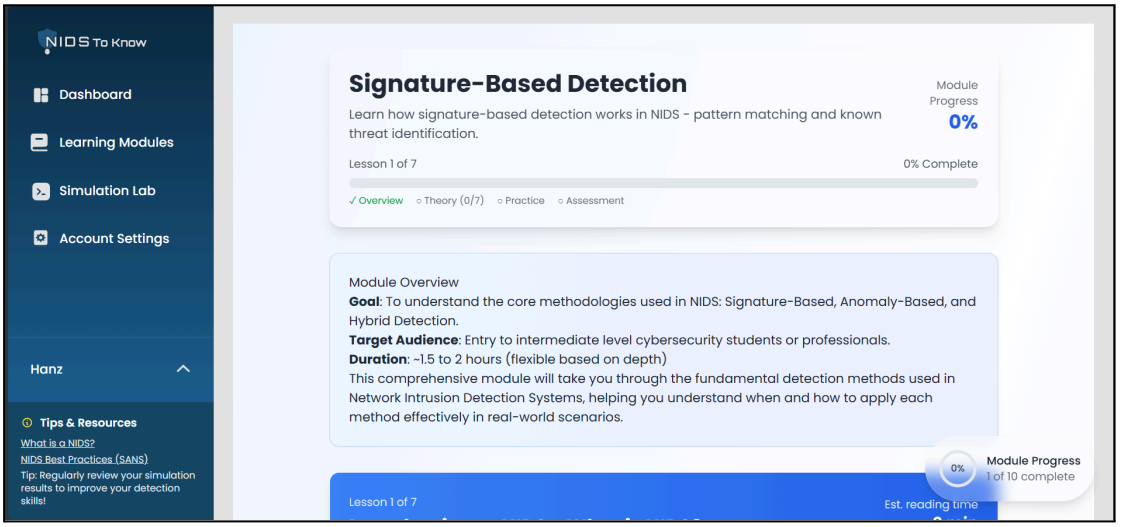

Figure 1. *Signature-based Module*

Figure 1 shows the Anomaly-Based Detection module, which examines

abnormal activities in network traffic by comparing them to established norms. Learners are introduced to its main concepts, key characteristics, and illustrative scenarios that explain how this method detects suspicious behavior within NIDS.

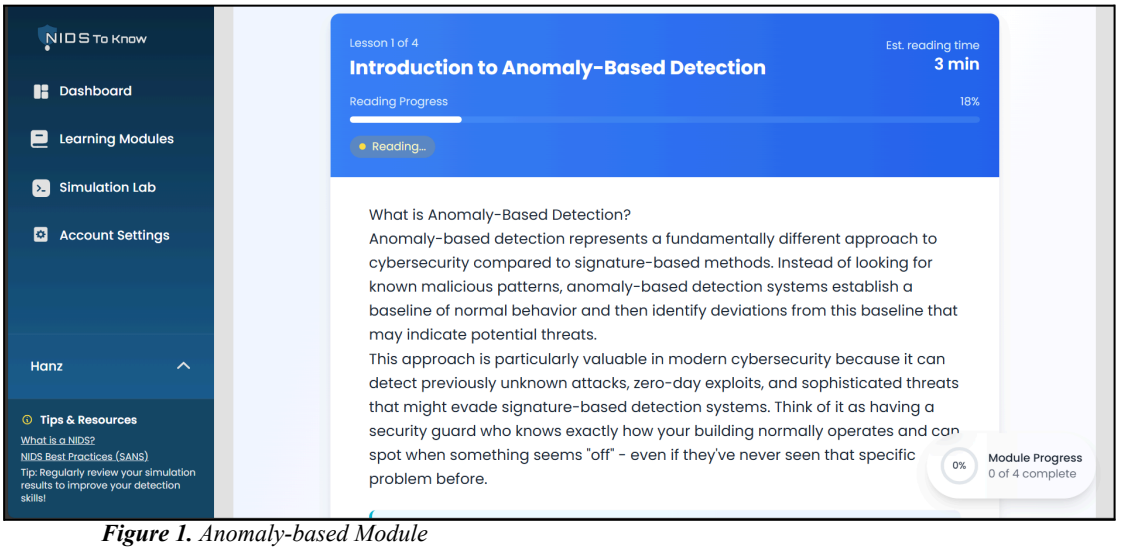

Figure 1. *Anomaly-based Module*

Figure 1 shows the Hybrid Detection module, which combines signature-based and anomaly-based techniques to improve accuracy in identifying network threats. It gives learners a clear overview and examples of how both methods work together in NIDS.

Figure 1. *Hybrid Module*

Traditional education including the cybersecurity often relies on passive, theory-heavy approaches that limit student engagement and hinder the development of practical skills (Yang et al., 2023). To address this issue, the system integrates an interactive simulation component developed with the Cowrie Honeypot, which emulates SSH and Telnet environments commonly targeted by attackers, and provides a built-in Linux terminal where students can simulate commands typically used in intrusion attempts. Studies have shown that interactive simulations enhance learning outcomes by enabling students to apply theoretical concepts in realistic, hands-on scenarios, thereby improving engagement, comprehension, and skill retention (Musa et al., 2023). As illustrated in Figure 1, the signature-based terminal applies the Aho-Corasick Algorithm to match entered commands with known attack patterns; when a match is detected, the activity is flagged as malicious, and live detection results are displayed, allowing learners to immediately observe threats and understand the practical application of detection methods, which directly addresses the limitations of passive, theory-driven training.

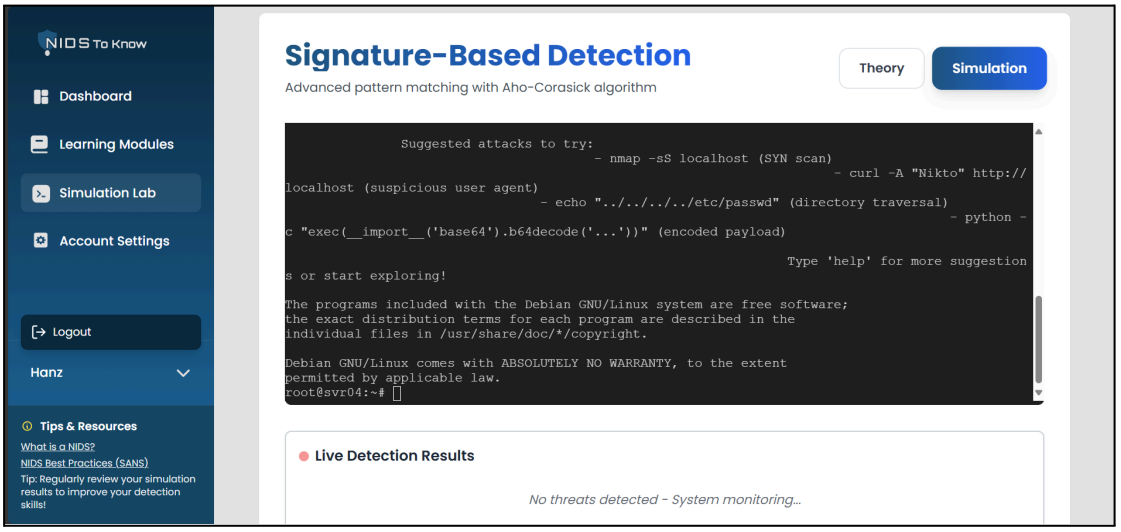

Figure 1. *Signature-based Interactive Simulation Terminal*

Figure 1 shows the anomaly-based terminal, where the system uses the

Isolation Forest algorithm to detect unusual commands that deviate from normal behavior. If suspicious activity is identified, it is flagged as malicious, and a live detection result is displayed on the interface. For anomaly-based detection, the system further classifies the level of threat into low, medium, or high, allowing learners to understand the severity of the detected activity.

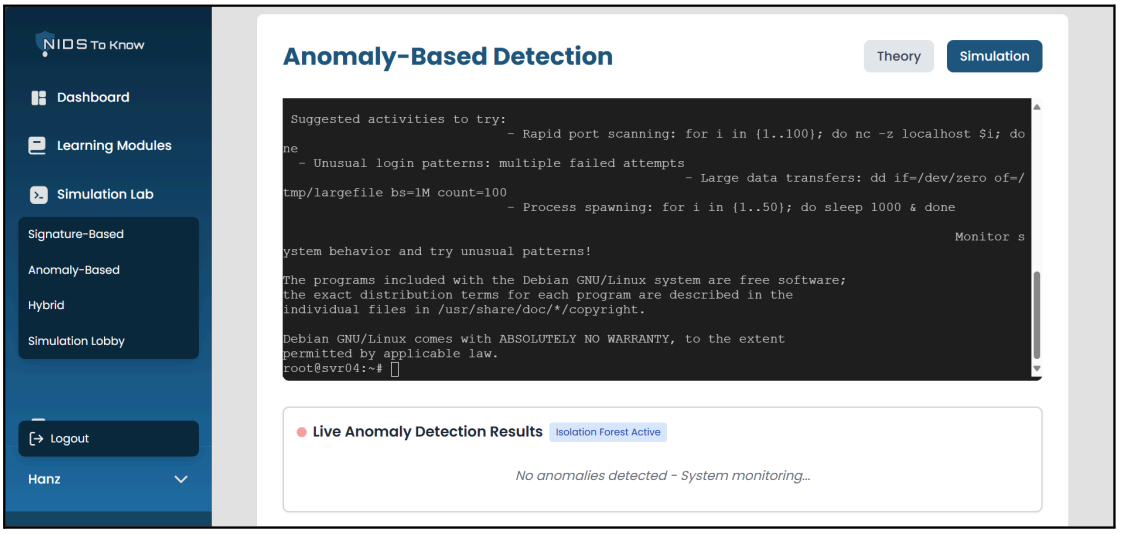

Figure 1. *Anomaly-based Interactive Simulation Terminal*

Figure 1 illustrates the hybrid terminal, where both signature and anomaly detection work together to evaluate commands. If harmful behavior is identified, the outcome is instantly displayed, allowing students to observe how the dual approach strengthens detection. The system also indicates the seriousness of the intrusion by labeling it with a corresponding threat level, enhancing the learner's understanding of its risk.

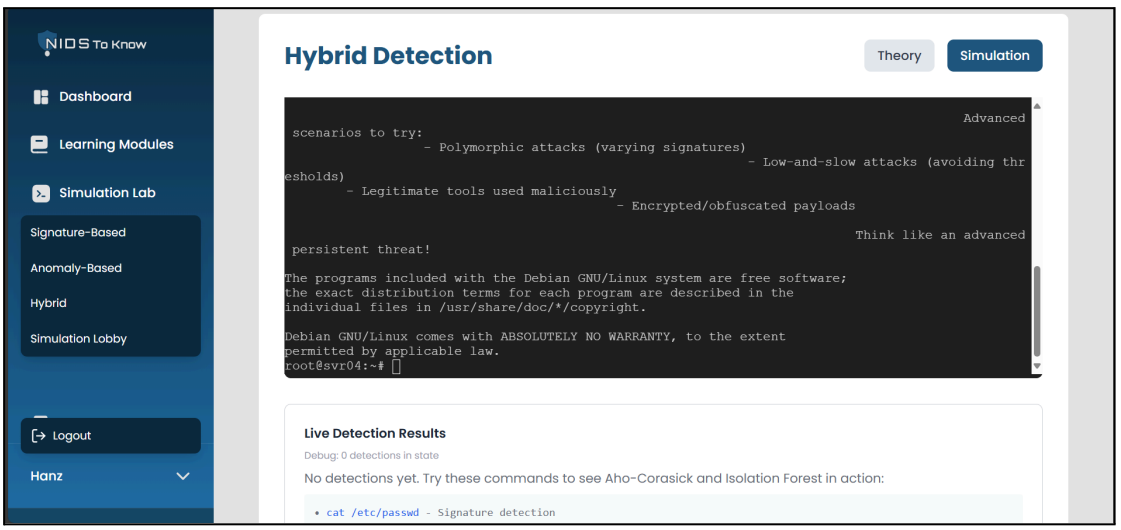

Figure 1. *Hybrid Interactive Simulation Terminal*

To provide a practical simulation in attacker–defender setting

Many traditional cybersecurity learning approaches focus on individual tasks and provide limited opportunities for collaboration, which restricts the development of teamwork and role specialization skills essential for real-world cyber defense (Buchler et al., 2018; Alahmari et al., 2022). As shown in Figure 1, the researchers added a simulation lobby to serve as the entry point for the practical attacker–defender activity. The customized code for session access can be created by the instructor. There is also a chat feature that helps participants interact even before the simulation and during the simulation. Anytime the participants are set, the instructor can commence the session and control the instructor in charge of the session can control the activity during the session. Having this feature in the platform, simulation based training provides learners with the effective procedures to enhance skill acquisition and outcomes in real world situations (Elendu et al., 2024).

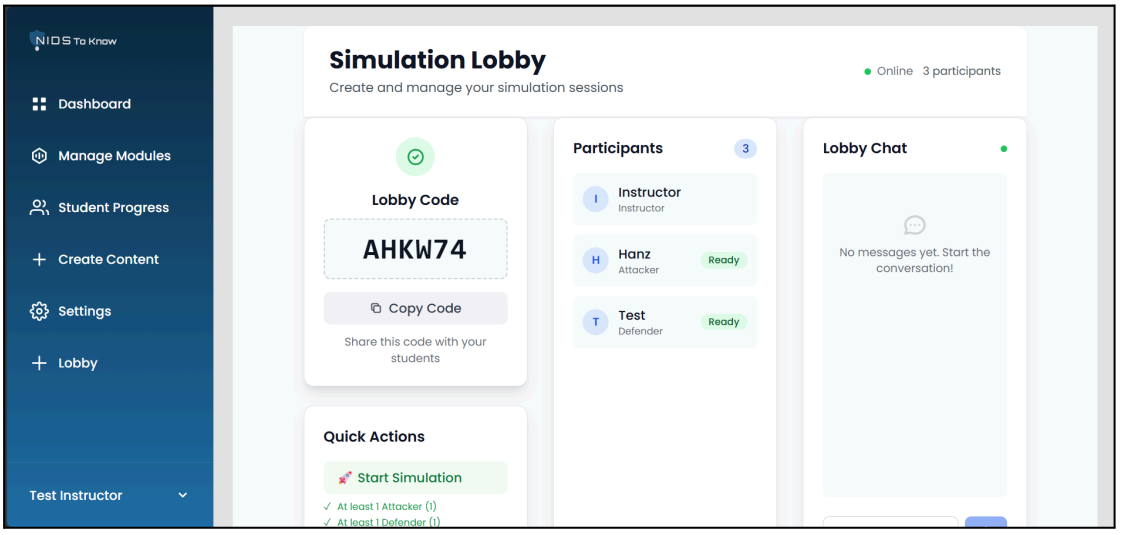

Figure 1. *Simulation Lobby*

The attacker's role was designed to simulate intrusion attempts within a controlled environment using the embedded Linux terminal integrated with the

Cowrie Honeypot. A significant number of learners struggle to grasp how attackers function, and this lack of attacker-focused knowledge hinders their capacity to predict tactics and build effective defense strategies (Morić, 2025). As displayed in Figure 1, attackers are tasked to accomplish specific attack objectives within a given time limit by executing commonly used hacking commands. Each completed objective corresponds to a set of points, while detection alerts provide feedback regarding the system's response. The point-based system encourages attackers to plan their strategies under time limits, simulating realistic attack scenarios. Studying attacker behavior, as emphasized by Shinde and Doshi (2025), can help identify these strategies and, in turn, strengthen defensive measures.

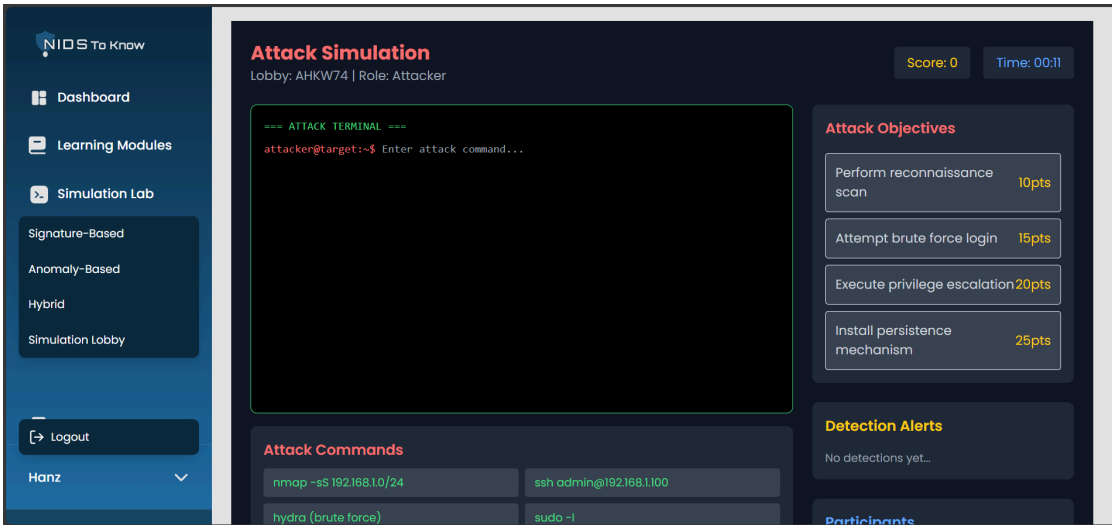

Figure 1. *Attacker Panel*

Current cybersecurity platforms lack sufficient opportunities for defenders to engage in real-time threat analysis and decision-making, leaving them underprepared to address evolving attacks (Shin et al., 2024). As shown in Figure 1, the defender panel provides access to a live detection feed that displays total events, identified threats, blocked attacks, and false positives. Defenders can also block suspicious IP addresses and configure detection algorithms such as Aho-Corasick, Isolation Forest,

or both in hybrid mode. Their main task is to accurately identify attacker activities within the set time frame, with points awarded for effectively analyzing and responding before attackers achieve their goals. According to Zielinski and Kholidy (2022), honeypots like Cowrie allow defenders to observe attacker behaviors and gain valuable insights into attack methods and defensive strategies.

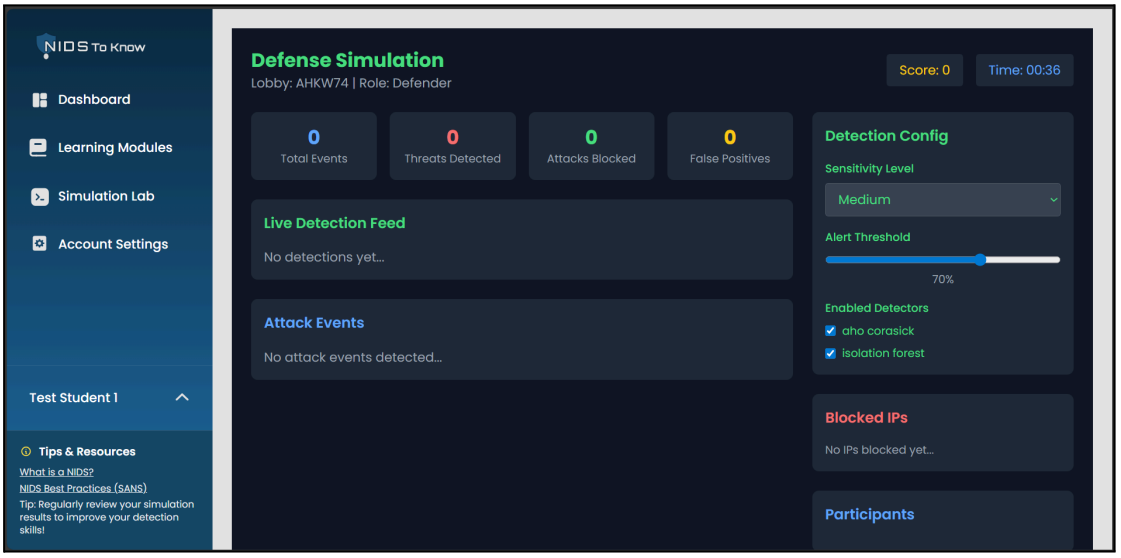

Figure 1. *Defender Panel*

The instructor panel was developed by the proponents to provide monitoring and control capabilities, enabling instructors to oversee attacker and defender activities, adjust difficulty levels, manage simulation time, and provide optional hints. As shown in Figure 1, it also offers tools such as live participant tracking, reporting, screenshots, and data export for documentation and evaluation. These features directly respond to a common limitation in cybersecurity training platforms, where instructors often lack real-time oversight and flexibility to adapt scenarios to participants' needs (Nespoli et al., 2024). Real-time monitoring has been shown to enhance training effectiveness by allowing instructors to evaluate performance and dynamically adjust scenarios to improve learning outcomes (Zhao et al., 2024).

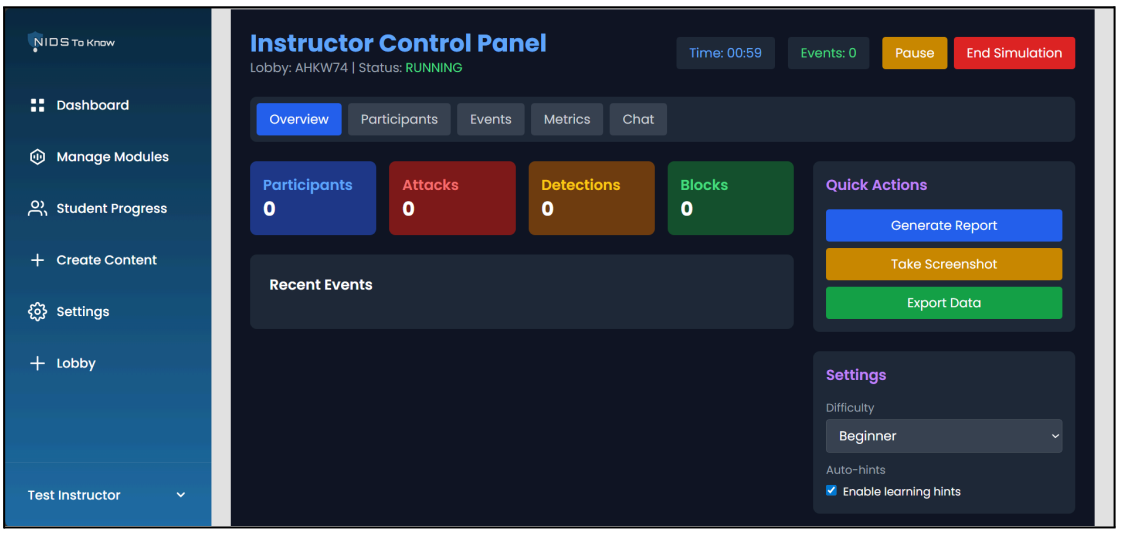

Figure 1. *Instructor Panel*

To equip instructors with tools to assign modules, monitor learner engagement, and deliver feedback.

Given the current generation's growing need for technology-based education, many universities view digital tools as crucial for supporting their management and instructional procedures (Palve & Palve, 2023). In line with this trend, the proponents implemented an assign module feature to assist instructors in their tasks. As shown in the *figure*, instructors have the freedom to view and manage the modules distributed to every student along with details such as description, current status, number of enrolled students, and last update date. Instructors can use the Assign action to give each student a module by selecting their name, setting an optional due date, and adding a customized remark or instructions. When it's finished, the system will let them know that the module was successfully allocated. This feature not only simplifies the assignment of modules but also enhances efficiency by automating repetitive manual tasks, resulting in a lighter workload for instructors (Tessitore, 2024).

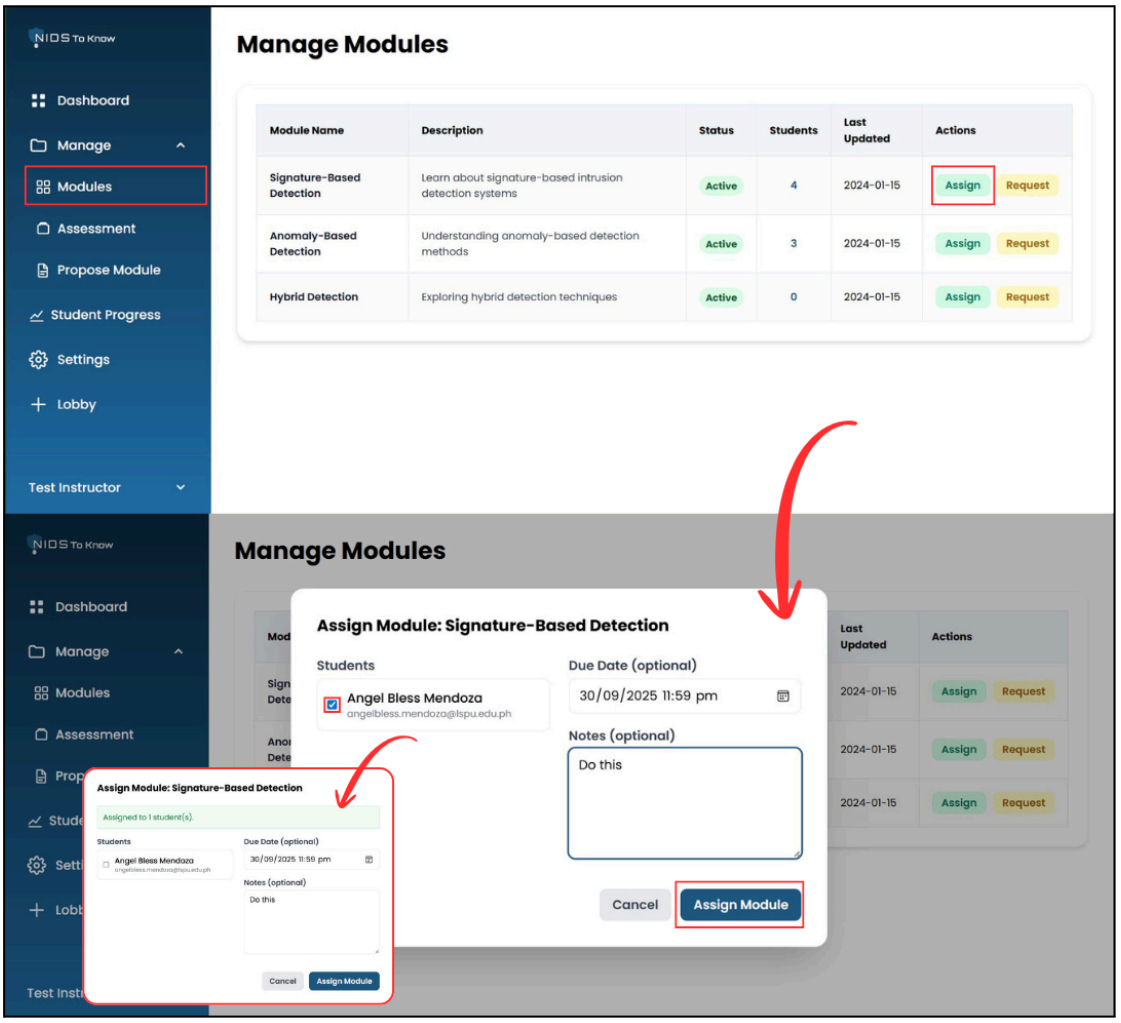

Figure 1. *Instructor's Module Assignment*

Figure illustrates student progress in the instructor's dashboard, indicating that student progress monitoring has been implemented. This feature gives instructors essential indicators such as overall progress, completed modules, and last active date. It enables instructors to quickly identify students who are progressing well, those who have low completion, and those who have been inactive. In addition, a search bar is provided at the top corner, allowing instructors to quickly locate and monitor a specific student. As Vaccaro and Sabella (2018) mentioned, monitoring student progress plays a vital role in academic growth, as it allows instructors to identify areas where students are struggling. Similarly, Lee et al., (2024) found that instructors

perceived monitoring student engagement as a valuable tool enabling them to adjust their teaching dynamically to meet the varying needs of students, thereby ensuring that learning gaps are addressed promptly and overall learning outcomes are improved.

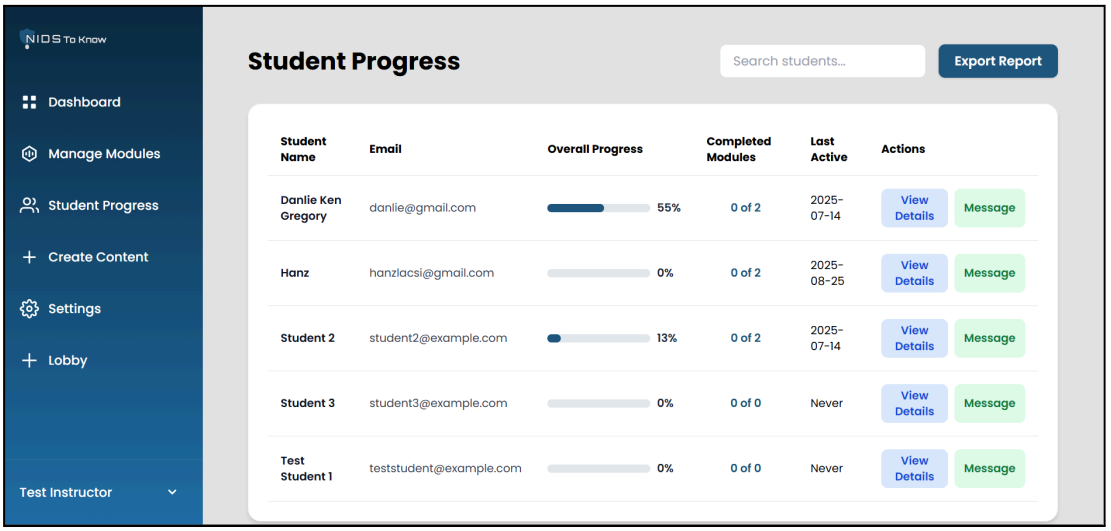

Figure 1. *Student Progress*

Feedback is considered an essential part of learning because it involves comprehensive understanding, timeliness, motivation, and usefulness (Zahid & AlManiam, 2025). Recognizing this importance, the system incorporates a delivery feedback feature that simplifies communication between instructors and students. As shown in the figure, instructors are able to give feedback directly within the platform by selecting the feedback button next to each student's task, which opens a feedback panel for writing comments or guidance. This feature reduces the use of a third-party platform and ensures that all feedback is centralized and accessible. Furthermore, the system enhances the feedback process by allowing instructors to provide immediate, targeted responses.

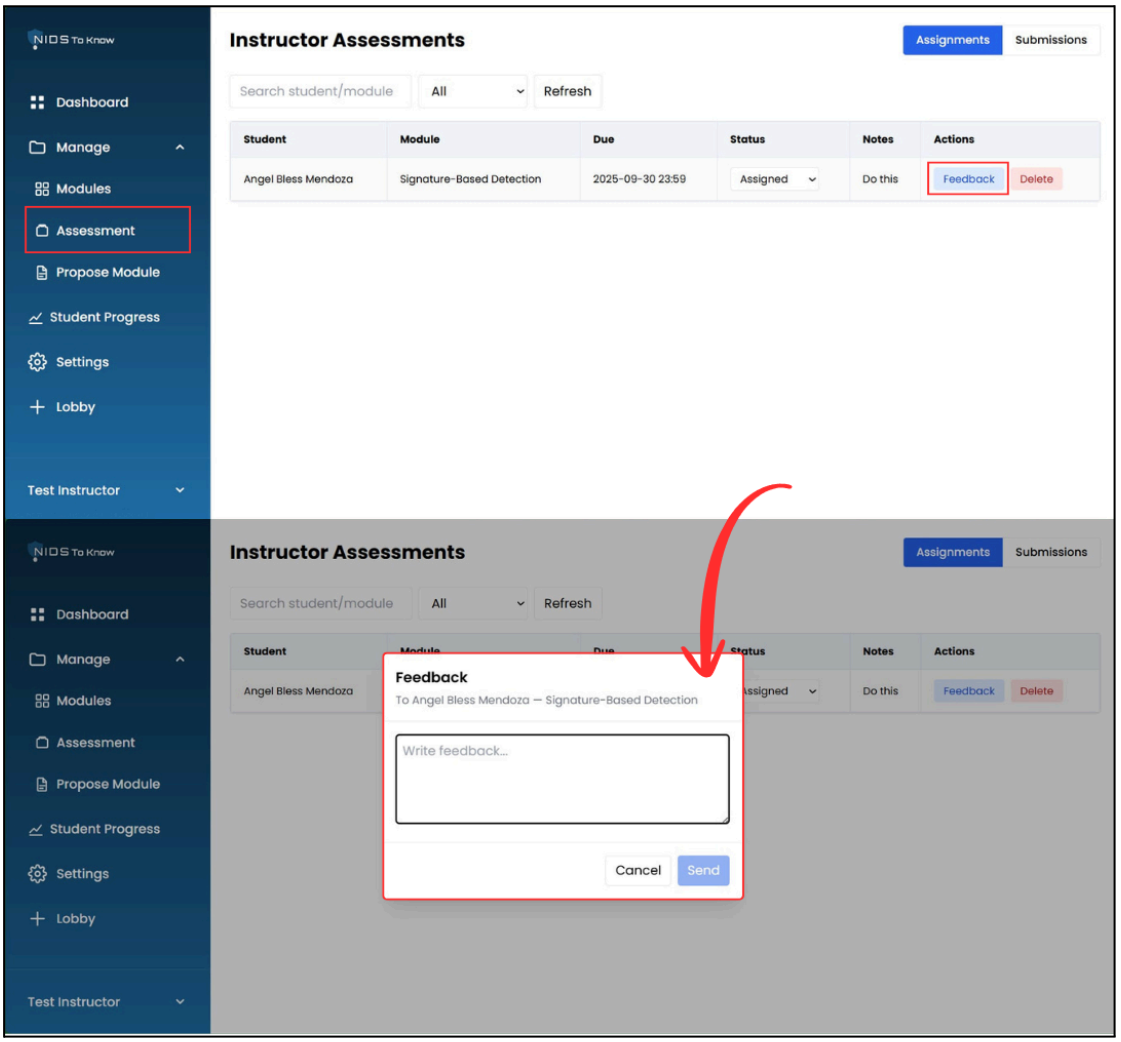

***Figure 1**. Instructor Assessments*

To utilize Aho-Corasick Algorithm (ACA) for signature-based, Isolation Forest Algorithm (IFA) for anomaly-based, and both ACA and IFA for hybrid.

The utilization of detection algorithms was successfully implemented in the NIDStoKnow platform to support signature-based, anomaly-based, and hybrid approaches. The Aho-Corasick Algorithm (ACA) was integrated for signature-based detection, enabling the system to efficiently match predefined attack patterns against user-simulated commands. For anomaly-based detection, the Isolation Forest

Algorithm (IFA) was applied to identify unusual or abnormal behaviors by analyzing command patterns that deviate from normal activity. A hybrid detection mode was also developed by combining ACA and IFA, allowing the system to benefit from both precise signature matching and behavioral anomaly identification. In this mode, detection outcomes are further classified into low, medium, or high levels of severity, providing a clearer assessment of the potential risks. The successful integration of these algorithms ensures that the platform can demonstrate the distinct strengths of different NIDS methods, offering students a practical understanding of how signature-based, anomaly-based, and hybrid detection operate in real-world scenarios.

To implement role-based access control (RBAC) for learners, instructors, and administrators to manage access to platform features based on user roles.

The implementation of Role-Based Access Control (RBAC) in the platform regulates access to system functionalities for students, instructors, and administrators. Through this mechanism, each user role is defined by a distinct set of privileges and responsibilities, ensuring that the interaction with the platform remains secure, organized, and function-oriented. During the sign up process, users are prompted to select their account type—either student or instructor—which determines the level of access they are granted within the system. For instance, students are provided with access to theoretical modules and simulation activities, while instructors are given additional tools for monitoring learner engagement, managing modules, and providing feedback. Administrators, on the other hand, are entrusted with system-level settings, user management, and security monitoring, accessible only through verified credentials. This structured role assignment not only secures sensitive components of

the platform from unauthorized access but also optimizes the overall user experience by presenting features that are relevant to each role (Ratna et al., 2025). As a result, the use of RBAC in the NIDSToKnow platform ensures both functionality and integrity, aligning with the project's objective of delivering a secure and efficient learning environment for network intrusion detection systems.

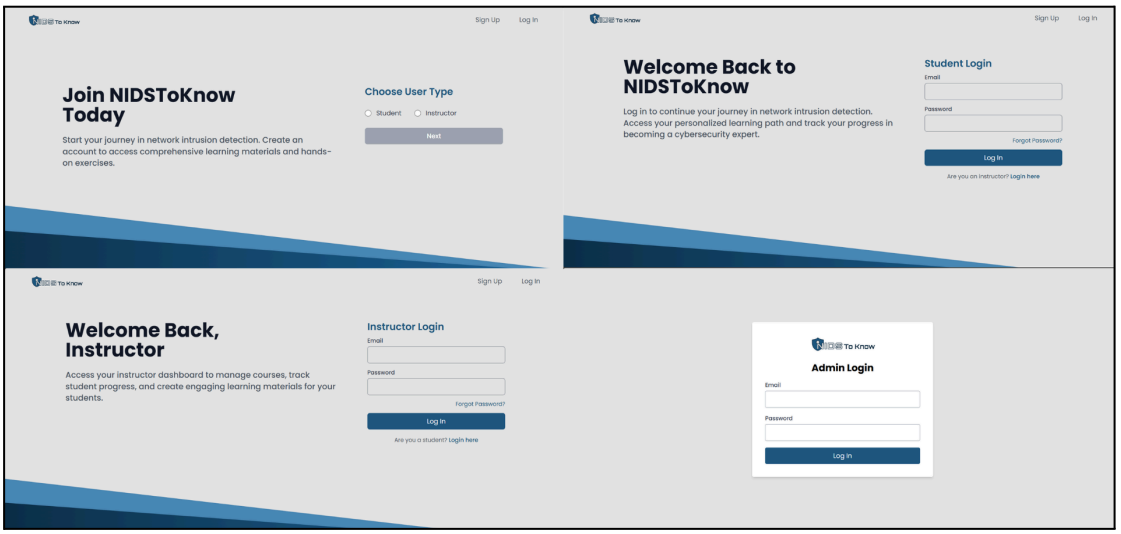

Figure 1.

After logging in, users are directed to a role-specific dashboard that reflects the implementation of the RBAC structure. For students, the dashboard highlights indicators such as overall progress, average progress across all components, total time spent on learning, and an engagement score, all of which help students assess their level of commitment and performance. To provide a clearer representation of their achievements and areas that require improvement, a visual tool such as pie chart for module completion progress, a bar graph displaying assessment scores over time, and a simulation activity tracker are also included.

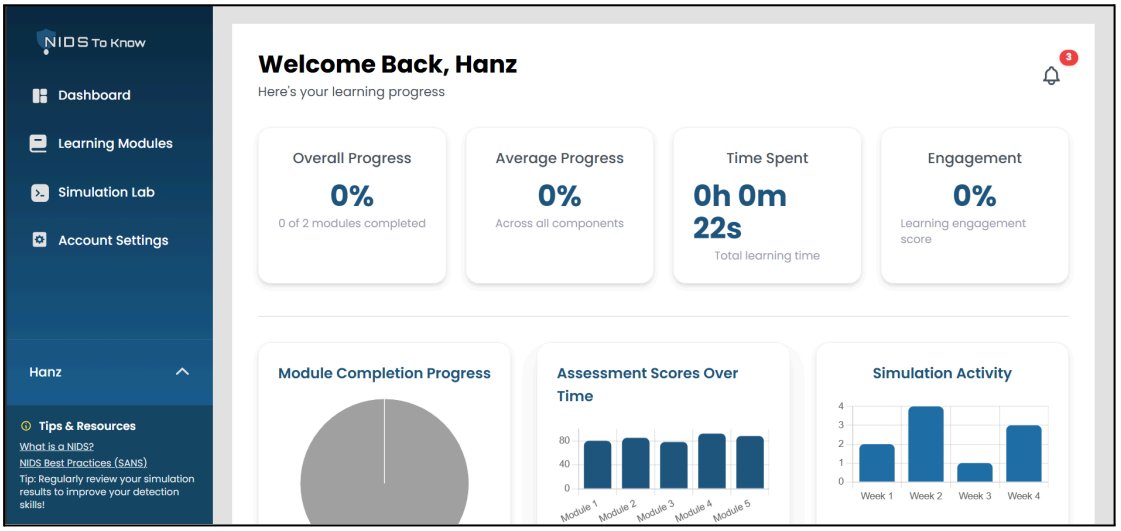

Figure 1. *Student Dashboard*

The instructor dashboard, as shown in the figure, provides instructors with essential insights and management tools to support teaching and monitoring functions. It displays key metrics such as the total number of students, active modules, average completion rate, and recorded feedback, enabling instructors to assess overall class performance at a glance. Visual aids such as the student enrollment chart, module completion graph, and feedback trend tracker further enhance monitoring by providing a clear representation of engagement and progress. In addition, the dashboard equips instructors with the ability to oversee modules and student progress, allowing them to address learning gaps promptly and provide targeted support where needed.

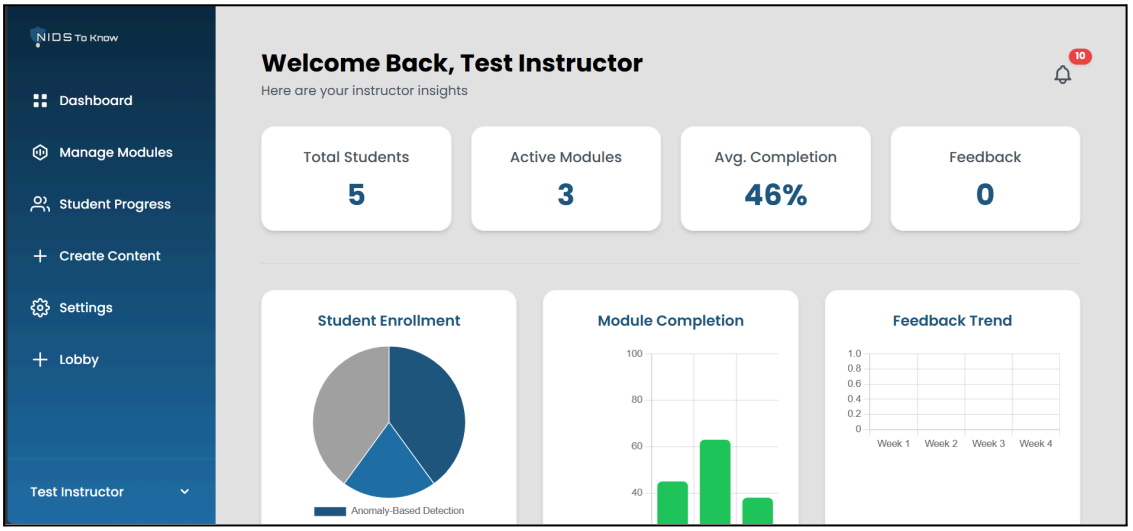

Figure 1. *Instructor Dashboard*

For administrators, the dashboard consolidates essential system management features into a clear and organized interface. It displays the total number of users, categorized into students and instructors, along with pending approval requests to facilitate account verification. The system status section provides real-time information on the platform's operational state, including API connectivity and database health, ensuring administrators can monitor technical stability. Additionally, quick actions such as user management and system settings are accessible for efficient oversight. A recent signups table is also included, showing newly registered users with details such as name, email, role, and approval status, further supporting effective account supervision.

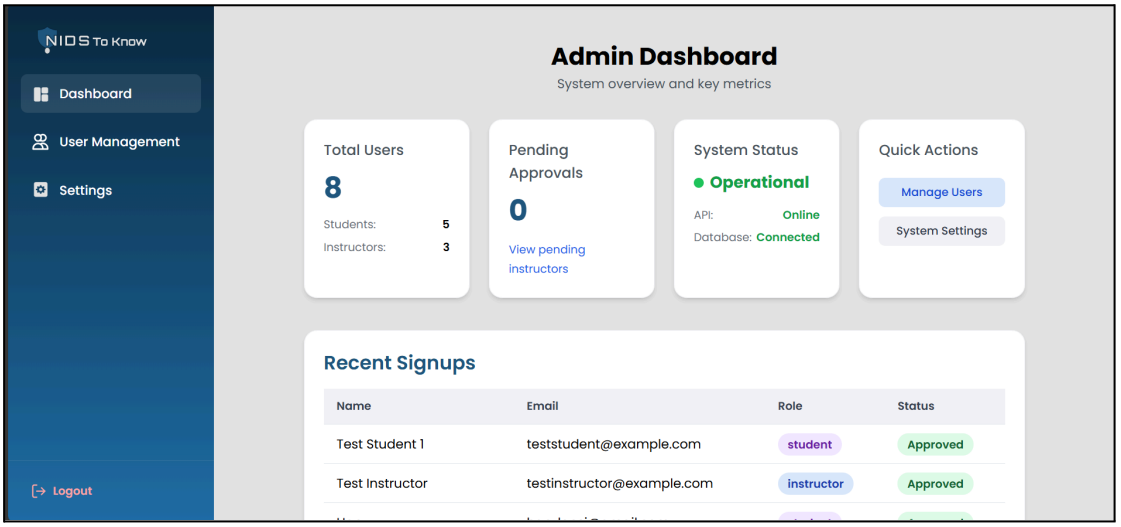

Figure 1. *Admin Dashboard*

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter includes a summary of the main findings of the study. It also presents the significance of the study, and relates findings to the objectives and problems written in the introduction part of the study. Recommendation/s must be stated in this chapter. This part usually directs the reader to conduct further research on some specific areas related to the study.

Summary

This section presents the summary of the results of the research study. Should isolate all the important points, review all the ideas on your list. Summary does not require you to critic you just summarize the content briefly in order to establish for the reader the ideas of the study.

Conclusions

This section presents the based on the objectives and merge with the finding of the study.

Recommendation

This section presents based on the conclusions, may include further research of the study. It may also include a direction on how to use the software product in order to achieve maximum benefits.

REFERENCES

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics, 8(3), 322. https://doi.org/10.3390/electronics8030322

Aho, A. V., & Corasick, M. J. (1975). Efficient string matching: An aid to bibliographic search. Communications of the ACM, 18(6), 333–340.

Alawida, M., Shawar, B., Abiodun, O., Mehmood, A., Omolara, A., & Hwaitat, A. (2024). Unveiling the dark side of chatgpt: exploring cyberattacks and enhancing user awareness. Information, 15(1), 27. https://doi.org/10.3390/info15010027

Al‐Balushi, S. and Martin‐Hansen, L. (2019). The development of students' justifications for their positions regarding two theoretical models: electron cloud or sodium chloride crystal after engaging in different learning activities. Journal of Research in Science Teaching, 56(8), 1011-1036. https://doi.org/10.1002/tea.21535

AlSanad, J. H. (2024). Cybersecurity in education. International Journal of Computer Science and Information Technology Research, 12(2), 51–61. https://doi.org/10.5281/zenodo.12566761

Anderson, T. (2008). The theory and practice of online learning (2nd ed.). Athabasca University Press.

Aoyama, D., Yonemura, K., & Shiraki, A. (2024). Effective methods in cybersecurity education for beginners. In Proceedings of the 2024 12th International Conference on Information and Education Technology (ICIET) (pp. 372–375). IEEE. https://doi.org/10.1109/ICIET60671.2024.10542828

Asif, M. K., Khan, T. A., Taj, T. A., Naeem, U., & Yakoob, S. (2013). Network intrusion detection and its strategic importance. Department of Electrical Engineering, King Saud University; University of Malaya.

Azizan, A., Mostafa, S., Mustapha, A., Foozy, C., Wahab, M., Mohammed, M., … & Khalaf, B. (2021). A machine learning approach for improving the performance of network intrusion detection systems. Annals of Emerging Technologies in Computing, 5(5), 201-208. https://doi.org/10.33166/aetic.2021.05.025

Az-zahra, F., Lukman, H., & Balkist, P. (2023). Development of pbl-based mathematics teaching modules to improve the mathematical critical thinking skills of elementary school students. Jurnal Inovasi Matematika, 5(2), 131-150. https://doi.org/10.35438/inomatika.v5i2.392

Back, S., LaPrade, J., & Soor, S. (2018). Spatial and temporal patterns of cyberattacks: effective cybercrime prevention strategies around the globe. J-Institute, 3(1), 7-13. https://doi.org/10.22471/protective.2018.3.1.07

Banik, S. and Peña, L. (2015). Deploying agents in the network to detect intrusions.. https://doi.org/10.1109/icis.2015.7166574

Begley, K., Monaghan, M., & Qi, Y. (2013). Repeated testing to improve skills in a pharmacy practice laboratory course. American Journal of Pharmaceutical Education, 77(6), 130. https://doi.org/10.5688/ajpe776130

Bernhardsson, L., Gellerstedt, M., & Winman, T. (2017). Work-integrated-learning: so, what? a framework for describing the level of integration between work and learning.. https://doi.org/10.21125/iceri.2017.0165

Bishop, C. M. (1995). Neural Networks for Pattern Recognition. Oxford University Press.

Bond, J. G. (2017). Introduction to game design, prototyping, and development. Addison-Wesley Professional.

Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, 93–104.

Carrillo-Mondejar, J., Carrillo-Mondejar, J., Roldán-Gómez, J., Gómez, S., & Villafranca, G. (2024). Stories from a customized honeypot for the IoT. https://doi.org/10.53106/160792642024012501010

Chabchoub, Y., Togbe, M. U., Boly, A., & Chiky, R. (2022). An in-depth study and improvement of Isolation Forest. IEEE Access, 10, 10219–10237.

Chua, W., Pajas, A. L. D., Castro, C. S., Panganiban, S. P., Pasuquin, A. J., Purganan, M. J., Malupeng, R., Pingad, D. J., Orolfo, J. P., Lua, H. H., & Velasco, L. C. (2024). Web traffic anomaly detection using Isolation Forest. Informatics, 11(4), 83. https://doi.org/10.3390/informatics11040083

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Croft, D. (2018). Embedding constructive alignment of reading lists in course design. Journal of Librarianship and Information Science, 52(1), 67-74. https://doi.org/10.1177/0961000618804004

Cruz, L. and Rivera, K. (2022). Development and validation of project-based module for selected topics in biology. International Journal of Educational Research & Social Sciences.

De Ramos, N. M., & Esponilla, F. D. II. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education (IJERE), 11(3), 1198–1209. https://doi.org/10.11591/ijere.v11i3.22863

Department of Information and Communications Technology. (2022). National Cybersecurity Plan 2022. Republic of the Philippines. https://dict.gov.ph/national-cybersecurity-plan-2022

Duan, T., Tian, Y., Zhang, H., Liu, Y., Li, Q., Jiang, J., … & Shi, Z. (2020). Intelligent processing of intrusion detection data. Ieee Access, 8, 78330-78342. https://doi.org/10.1109/access.2020.2989498

Eniodunmo, O. and Al-Aqtash, R. (2023). A predictive model to predict a cyberattack using self normalizing neural networks. International Journal of Statistics and Probability, 12(6), 60. https://doi.org/10.5539/ijsp.v12n6p60

Farooq, M., Abbas, S., Rahman, A., Sultan, K., Khan, M., & Mosavi, A. (2023). A fused machine learning approach for intrusion detection system. Computers Materials & Continua, 74(2), 2607-2623. https://doi.org/10.32604/cmc.2023.032617

Ferm, L. (2021). Vocational students' ways of handling the academic/vocational divide. International Journal for Research in Vocational Education and Training, 8(1). https://doi.org/10.13152/ijrvet.8.1.1

Garrison, D. R., & Kanuka, H. (2004). Blended learning: Uncovering its transformative potential in higher education. The Internet and Higher Education, 7(2), 95-105. https://doi.org/10.1016/j.iheduc.2004.02.001

Gestwicki, P., & Stumbaugh, K. (2015). Educational games for cybersecurity: A review. In 2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES) (pp. 131–137).

Gudimetla, S. and Kotha, N. (2024). Enhancing threat detection and response strategies. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets55883

Ho, S., Al-Jufout, S., Dajani, K., & Mozumdar, M. (2021). A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. Ieee Open Journal of the Computer Society, 2, 14-25. https://doi.org/10.1109/ojcs.2021.3050917

Holmgren, D., Nilsson, M., & Wekell, P. (2019). Combining learning for educators and participants in a paediatric cpd programme. BMC Medical Education, 19(1). https://doi.org/10.1186/s12909-019-1461-x

Ibraheem, I. (2022). Enhancing intrusion detection systems using ensemble machine learning techniques. Data & Metadata, 1, 33. https://doi.org/10.56294/dm202271

Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: A review. ACM Computing Surveys (CSUR), 31(3), 264–323.

Jain, J. & Waoo, A. (2023). An artificial neural network technique for prediction of cyber-attack using intrusion detection system. Journal of Artificial Intelligence Machine Learning and Neural Network, (32), 33-42. https://doi.org/10.55529/jaimlnn.32.33.42

Jain, Y. K., & Singh, S. (2011). Honeypot-based secure network system. International Journal on Computer Science and Engineering (IJCSE), 3(2), 615.

Knipp, C. T. (2006). Physics education research's study on the reliability and validity of exams. American Physics Journal, 10.

Koehler, R., Sharma, U., & Nord, P. (2024). Addressing the cybersecurity skills gap with higher education. IBM. https://www.ibm.com/new/announcements/addressing-cybersecurity-skills-gap-higher-education

Knorr, E. M., & Ng, R. T. (1998). Algorithms for mining distance-based outliers in large datasets. Proceedings of the 24th International Conference on Very Large Data Bases, 392–403.

Korda, D. and Dapaah, E. (2023). The role of cyberattacks on modern warfare: a review. International Journal of Research and Innovation in Applied Science, VIII(VII), 286-292. https://doi.org/10.51584/ijrias.2023.8733

Kumar, A., Gupta, S., Rai, A., & Sinha, S. (2013). A study on cybersecurity awareness and education. International Journal of Scientific and Research Publications, 3(6), 1–5.

Kumar, S., Gupta, S., & Arora, S. (2021). Research trends in network-based intrusion detection systems: A review. IEEE Access, 9, 140149–140173. https://doi.org/10.1109/ACCESS.2021.3129775

Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (lstm). Journal of Big Data, 8(1). https://doi.org/10.1186/s40537-021-00448-4

Lavrova, D. (2025). Cybersecurity threatscape in Southeast Asia. PositiveTechnology. https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-southeast-asia

Ledezma, C., Font, V., & Sala, G. (2022). Analysing the mathematical activity in a modelling process from the cognitive and onto-semiotic perspectives. Mathematics Education Research Journal, 35(4), 715-741. https://doi.org/10.1007/s13394-022-00411-3

Lee, C. and Sen, A. (2018). Students voice in their learning: incorporating students' expectations in learning design of e-learning of pharmacotherapy. International Journal of Learning and Teaching, 203-208. https://doi.org/10.18178/ijlt.4.3.203-208

Liangxu, S., & Linlin, L. (2012). Improve Aho-Corasick algorithm for multiple patterns matching memory efficiency optimization. Journal of Convergence Information Technology, 7(19), 173–179. https://doi.org/10.4156/jcit.vol7.issue19.19

Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. 2008 Eighth IEEE International Conference on Data Mining, 413–422. https://doi.org/10.1109/ICDM.2008.17

Liu, Q., He, Y., & Yang, S. H. (2018). Journal of Chongqing University (Social Science Edition), 5, 218–226.

Mäkelä, M., Sarvelainen, H., & Lyytikäinen, T. (2018). Learning heat dynamics using modelling and simulation.. https://doi.org/10.3384/ecp17142403

Maraj, A., Sutherland, C., & Butler, W. (2021). The challenges to cybersecurity education in developing countries: A case study of Kosovo. AAB College, Faculty of Computer Sciences; Capitol Technology University.

Martini, B., & Choo, K. K. R. (2014). Cloud storage forensics: OwnCloud as a case study. In Proceedings of the Twenty Second European Conference on Information Systems.

Martini, B., & Choo, K. K. R. (2014). Proceedings of the Twenty-Second European Conference on Information Systems.

Masaguni, A., Lamangantjo, C., Katili, N., Pikoli, M., Buhungo, T., & Payu, C. (2023). Development of science learning modules based on project based leraning on additives and addictive substances (a research in class viii smp negeri 7 telaga biru). Jurnal Penelitian Pendidikan Ipa, 9(12), 10758-10767. https://doi.org/10.29303/jppipa.v9i12.5731

Mispriatin, M., Ginting, J., & Arifwidodo, B. (2022). Analisis kinerja honeypot dionaea dan cowrie dalam mendeteksi serangan. Prosiding Seminar Nasional Teknoka, 6, 170-178. https://doi.org/10.22236/teknoka.v6i1.448

MixMode Threat Research. (2024). Global cybercrime report 2024: Which countries face the highest risk? MixMode. https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/

Morić, Z., Mršić, L., Kunić, Z., & Đambić, G. (2024). Honeypots in cybersecurity: their analysis, evaluation and importance.. https://doi.org/10.20944/preprints202408.0946.v1

Naik, N., Shang, C., Jenkins, P., & Shen, Q. (2020). Building a cognizant honeypot for detecting active fingerprinting attacks using dynamic fuzzy rule interpolation. Expert Systems, 38(5). https://doi.org/10.1111/exsy.12557

National Cyber Security Index. (2023). Archived data from 2016-2023. https://ncsi.ega.ee/country/ph_2022/

Omictin, E. O. III, Gante, R. Jr., Villaflores, R. R. P., Marchan, M. B. C. M., & Noblefranca, R. T. Jr. (2023). The study on the applicability of Aho-Corasick algorithm in identifying tests' validity. Silliman University Research Repository.

Omonije, A. (2024). Agile methodology: A comprehensive impact on modern business operations. *International Journal of Science and Research (IJSR), 13*(2). https://doi.org/10.21275/SR24130104148

Priyanto, C. Y., Hendry, & Purnomo, H. D. (2021). Combination of Isolation Forest and LSTM Autoencoder for Anomaly Detection. 2021 2nd International Conference on Innovative and Creative Information Technology (ICITech), 35–38.

Qi, G., Chen, Z., Zhao, H., & Chensheng, W. (2019). Construction and application of machine learning model in network intrusion detection.. https://doi.org/10.2991/pntim-19.2019.83

Qin, J. L., & Leng, H. L. (2022). Application and exploration of gamification in cybersecurity education. Journal of Guangxi College of Education, 2, 144–151.

Republic of the Philippines. (2012). Republic Act No. 10175: An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes. The Lawphil Project. https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

Richey, R. C., & Klein, J. D. (2014). Design and Development Research. In Handbook of Research on Educational Communications and Technology (pp. 141-150). New York, NY: Springer.

Rousseeuw, P. J., & Leroy, A. M. (1987). Robust Regression and Outlier Detection. John Wiley & Sons.

S, D., & Chakkaravarthy, S. (2023). Containerized cloud-based honeypot deception for tracking attackers. Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-28613-0

Salazar, M., Gaviria, J., Laorden, C., et al. (2013). Enhancing cybersecurity training through immersive technologies. In 2013 IEEE Global Engineering Education Conference (EDUCON) (pp. 602–607).

Sayed, M. and Taha, M. (2023). Oblivious network intrusion detection systems.. https://doi.org/10.21203/rs.3.rs-3232596/v1

Seaman, J. E., Allen, I. E., & Seaman, J. (2018). Grade increase: Tracking online education in the United States. Babson Survey Research Group.

Setianto, F., Tsani, E., Sadiq, F., Domalis, G., Tsakalidis, D., & Kostakos, P. (2021). GPT-2C: A GPT-2 parser for Cowrie honeypot logs. https://doi.org/10.48550/arxiv.2109.06595

Sivanantham, S., Mohanraj, V., Suresh, Y., & Senthilkumar, J. (2023). Association rule mining frequent-pattern-based intrusion detection in network. Computer

Systems Science and Engineering, 44(2), 1617-1631. https://doi.org/10.32604/csse.2023.025893

Song, Z., Hong, Y., & Palaoag, T. (2022). An intelligent cyber security detection and response platform. International Journal for Research in Advanced Computer Science and Engineering, 8(12), 1-10. https://doi.org/10.53555/cse.v8i12.2167

Stephen, G. (1994). String searching algorithms. World Scientific Publishing.

Suratnu, R. (2023). The adoption of the addie model in designing an instructional module: the case of malay language remove students. International Journal of Indonesian Education and Teaching, 7(2), 262-270. https://doi.org/10.24071/ijiet.v7i2.3521

Susanti, R., Muhammad, A., & Prabowo, W. (2022). Implementasi intrusion prevention system (ips) ossec dan honeypot cowrie. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 11(1), 73-78. https://doi.org/10.32736/sisfokom.v11i1.1246

Tan, K. M. C., Killourhy, K. S., & Maxion, R. A. (2002). Undermining an anomaly-based intrusion detection system using common exploits. International Symposium on Recent Advances in Intrusion Detection, 54–73.

Thanh, N. (2020). Promoting learner autonomy through self-assessment and reflection. Vnu Journal of Foreign Studies, 35(6). https://doi.org/10.25073/2525-2445/vnufs.4483

Tinnaluri, V. and Shaik, N. (2024). A comprehensive approach: developing a honeypot system to thwart cyber attackers. eatp. https://doi.org/10.53555/kuey.v30i5.4517

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupé, A., & Vigna, G. (2017). Large-scale evaluation of automated security education systems. In USENIX Workshop on Advances in Security Education (ASE 17).

Tsoy, A., Ten, S., & Rakhimova, A. (2023). Project-based learning technology in classes for technical and it-orientating groups: experience and results of implementation. E3s Web of Conferences, 460, 05016. https://doi.org/10.1051/e3sconf/202346005016

Vanin, P., Newe, T., Dhirani, L., O'Connell, E., O'Shea, D., Lee, B., … & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22), 11752. https://doi.org/10.3390/app122211752

Vikram. (2025). 12 best countries to study cyber security. Kanan.co. https://www.kanan.co/blog/best-countries-to-study-cyber-security/

Wang, H., Morić, J., & Ng, D. (2022). Automating attack detection with machine learning techniques for honeypots. Computers & Security, 106, 102365. https://doi.org/10.1016/j.cose.2021.102365

Xiao, H., Wei, H., Liao, Q., Ye, Q., Cao, C., & Zhong, Y. (2023). Exploring the gamification of cybersecurity education in higher education institutions: An

analytical study. SHS Web of Conferences, 166, 01036. https://doi.org/10.1051/shsconf/202316601036

Xiao, H., Wei, H., Liao, Q., Ye, Q., Cao, C., & Zhong, Y. (2023). Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. SHS Web of Conferences, 166, 01036. https://doi.org/10.1051/shsconf/202316601036

Yeboah-Ofori, A., Mouratidis, H., Ismai, U., Islam, S., & Papastergiou, S. (2021). Cyber supply chain threat analysis and prediction using machine learning and ontology., 518-530. https://doi.org/10.1007/978-3-030-79150-6_41

Zhang, Q., Liang, Z., Liu, W., Peng, W., Huang, H., Zhang, S., Chen, L., Jiang, K., & Liu, L. (2022). Landslide susceptibility prediction: Improving the quality of landslide samples by Isolation Forests. Sustainability, 14(24), 16692.

Ahmed, S. (2024). A systematic review of learning management systems in cybersecurity education. Journal of Cybersecurity Education, 12(1), 45–62. https://doi.org/10.1080/xxxx

Beauchamp, L. (2023). The role of cyber ranges in cybersecurity education: A review of simulation-based training. Journal of Information Security Education and Research, 9(2), 101–117. https://doi.org/10.1080/xxxx

National Institute of Standards and Technology. (2023). Range Learning Management System (RLMS). NIST. https://csrc.nist.gov

Prümmer, C., Langner, A., & Schmitt, C. (2024). Cybersecurity training approaches: A review of methods and technologies. Computers & Education, 200, 104777. https://doi.org/10.1016/j.compedu.2023.104777

Son, J., Stewart, B., & Xenos, M. (2012). A comparative study of virtual laboratory solutions in higher education. Journal of Computing in Higher Education, 24(3), 201–218. https://doi.org/10.1007/s12528-012-9051-3

The Impact of Virtual Laboratories. (2024). Virtualization in technical education. Education and Technology Review, 15(2), 55–68. https://doi.org/10.1080/xxxx

Ukwandu, E., Armstrong, C., & Clarke, N. (2020). Cyber ranges and test-beds: A review of their role in cybersecurity education. International Journal of Information Security Science, 9(3), 152–168. https://doi.org/10.1007/s10207-020-00501-8

Tirado-Olivares, S., Cózar-Gutiérrez, R., González-Calero, J. A., & Dorotea, N. (2024). Evaluating the impact of learning management systems in geographical education in primary school: An experimental study on the importance of learning analytics-based feedback. Sustainability, 16(7), Article 2616. https://doi.org/10.3390/su16072616

Alotaibi, R., & Alsubaie, M. (2021). Role-based access control for higher education systems: Enhancing security and privacy. International Journal of Advanced Computer Science and Applications, 12(8), 451–459. https://doi.org/10.14569/IJACSA.2021.0120855

Chen, L., & Crampton, J. (2012). Risk-aware role-based access control. Proceedings of the 7th International Conference on Availability, Reliability and Security, 262–267. https://doi.org/10.1109/ARES.2012.8

Crampton, J., & Khambhammettu, H. (2008). Delegation in role-based access control. International Journal of Information Security, 7(2), 123–136. https://doi.org/10.1007/s10207-008-0050-8

Dlamini, M. T., & Eloff, J. H. P. (2019). Role-based access control in the Internet of Things. South African Computer Journal, 31(1), 1–15. https://doi.org/10.18489/sacj.v31i1.567

Ferraiolo, D. F., Gilbert, D. M., & Lynch, N. (1995). An examination of federal and commercial access control policy needs. Proceedings of the 16th NIST-NCSC National Computer Security Conference, 107–116.

Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2015). Guide to attribute based access control (ABAC) definition and considerations (NIST Special Publication 800-162). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

Hu, V. C., & Kuhn, D. R. (2018). Role-based access control: Features and motivations. Proceedings of the 23rd ACM Symposium on Access Control Models and Technologies, 123–132. https://doi.org/10.1145/3205977.3205982

Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. IEEE Computer, 43(6), 79–81. https://doi.org/10.1109/MC.2010.155

Ni, Q., Bertino, E., & Lobo, J. (2007). An obligation model bridging access control policies and privacy policies. Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, 133–142. https://doi.org/10.1145/1278960.1278981

Sandhu, R. S., & Samarati, P. (1994). Access control: Principles and practice. IEEE Communications Magazine, 32(9), 40–48. https://doi.org/10.1109/35.312842

Xu, H., Zhang, X., & Wang, J. (2020). A hybrid access control model for enterprise applications. Future Generation Computer Systems, 108, 418–428. https://doi.org/10.1016/j.future.2020.02.030

Zhao, J., & Bai, G. (2018). Dynamic role-based access control in cloud computing. Future Generation Computer Systems, 79, 370–379. https://doi.org/10.1016/j.future.2017.09.048

Beuran, C., et al. (2018). CyTrONE: An integrated cybersecurity training framework combining attack-, analysis-, and defense-oriented exercises.

Čeleda, P., Vykopal, J., Švábenský, V., & Slavíček, K. (2020). KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems. arXiv. https://arxiv.org/abs/2004.11575

Kebande, V. R. (2024). The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education. arXiv. https://arxiv.org/abs/2404.04952

Oikonomou, N., et al. (2021). Design and Implementation of Multi-Cyber Range for Cyber Training and Testing. Applied Sciences. https://doi.org/10.3390/app122412546

Švábenský, V., Vykopal, J., Čermák, M., & Laštovička, M. (2018). Enhancing Cybersecurity Skills by Creating Serious Games*. arXiv. https://arxiv.org/abs/1804.03567

Topham, N., et al. (2016). Simulation framework for practical cyber security training in the public service. Security and Defence Quarterly.

Buenaventura Jr, L. A., Cubol, J. S., Pascual, M. A. C., Ubaldo, E. S., Sario, D. R. D., & Velasco, M. S. (2024). Cybersecurity awareness of college students in a private higher education institution. CGCI International Journal of Administration, Management, Education and Technology, 1(1). Retrieved from https://www.cgci-ijamet.org/index.php/cgciijamet/article/view/26

Oducado, R. M. F., Dinero, E. M. G., Fuentes, I. K. M., De la Peña, J. F. L., & Ermita, G. B. (2022). Cybersecurity skills of Filipino nursing students at a public tertiary institution. WVSU Research Journal, 11(2), 1–7. Retrieved from https://www.ejournals.ph/article.php?id=20187

Bondoc, E. B., & Malawit, G. T. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. Global Journal of Engineering and Technology Advances, 2(3), 016–021.

Yuhong, Y., Zhuo, S., & Monreal, R. N. (2024). Design of the network security architecture for smart campus in the Philippines. Journal of Knowledge Learning and Science Technology, 5(3), 17–26.

Hattie, J., & Timperley, H. (2007). The power of feedback. Review of Educational Research, 77(1), 81–112. https://doi.org/10.3102/003465430298487

Kaliisa, R., Misiejuk, K., López-Pernas, S., Khalil, M., & Saqr, M. (2023). Have learning analytics dashboards lived up to the hype? A systematic review of impact on students' achievement, motivation, participation and attitude. arXiv. https://doi.org/10.48550/arXiv.2306.04255

Lee, M., Michos, K., & Mavroudi, A. (2025). How instructors use learning analytics: The pivotal role of pedagogy. Journal of Computing in Higher Education. https://doi.org/10.1007/s12528-025-09432-w

Tirado-Olivares, S., Martín-Romera, A., & Merino-Fernández, J. (2024). LMS dashboards for monitoring student engagement: Impacts on feedback and performance. Computers & Education, 204, 104908. https://doi.org/10.1016/j.compedu.2023.104908

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Alotaibi, M. A., & Furnell, S. M. (2016). A review of using gaming technology for cyber-security awareness. Computers & Security, 59, 1–15. https://doi.org/10.1016/j.cose.2015.12.002

Tymoshchuk, D., Yatskiv, V., Tymoshchuk, V., & Yatskiv, N. (2024). Interactive cybersecurity training system based on simulation environments. Measuring and Computing Devices in Technological Processes, 3, 52–56. https://doi.org/10.31891/2219-9365-2024-79-7

Abuhassna, H., Al-Rahmi, W. M., Yahya, N., Zakaria, M. A. Z. M., Kosnin, A. B. M., & Darwish, M. (2020). Development of a new model on utilizing online learning platforms to improve students' academic achievements and satisfaction. International Journal of Educational Technology in Higher Education, 17(38), 1–23. https://doi.org/10.1186/s41239-020-00216-z

Mayer, R. E. (2021). Multimedia learning (3rd ed.). Cambridge University Press.

Clark, R. C., & Mayer, R. E. (2016). E-learning and the science of instruction (4th ed.). Wiley.

Musa, S. A., Rafiq, A., & Mohamed, S. (2023). Interactive simulation-based learning in cybersecurity education: Enhancing student engagement and knowledge retention. International Journal of Emerging Technologies in Learning (iJET), 18(4), 45–60. https://doi.org/10.3991/ijet.v18i04.34567

Yang, X., Yuan, J., & Zhao, J. (2023). A highly interactive honeypot-based approach to network threat management. Future Internet, 15(4), 127. https://doi.org/10.3390/fi15040127

Buchler, B. C., LaFleur, K., Rajivan, P., Marusich, L., & Hoffman, R. R. (2018). Cyber teaming and role specialization in a cyber security defense competition. Frontiers in Psychology, 9, 2133. https://doi.org/10.3389/fpsyg.2018.02133

Alahmari S, Renaud K, Omoronyia I. Moving beyond cyber security awareness and training to engendering security knowledge sharing. Inf Syst E-Bus Manage. 2023;21(1):123–58. doi: 10.1007/s10257-022-00575-2. Epub 2022 Oct 12. PMCID: PMC9555687.

Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics, 12(1), 14. https://doi.org/10.3390/informatics12010014

Shinde, A., & Doshi, P. (2025). Modeling Behavioral Preferences of Cyber Adversaries Using Inverse Reinforcement Learning. arXiv. https://arxiv.org/abs/2505.03817

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. Electronics, 13(19), Article 3867. https://doi.org/10.3390/electronics13193867

Zielinski, D., & Kholidy, H. A. (2022). An Analysis of Honeypots and their Impact as a Cyber Deception Tactic. arXiv. https://arxiv.org/abs/2301.00045

Nespoli, P., Albaladejo-González, M., Pastor Valera, J. A., Ruipérez-Valiente, J. A., Garcia-Alfaro, J., & Gómez Mármol, F. (2024). SCORPION Cyber Range: Fully customizable cyber-exercises, gamification, and learning analytics to train cybersecurity competencies. arXiv. https://arxiv.org/abs/2401.12594

Zhao, M., Jia, W., Jennings, S., Law, A., Bourgon, A., Su, C., Larose, M.-H., Grenier, H., Bowness, D., & Zeng, Y. (2024). Monitoring pilot trainees' cognitive control under a flight simulation training process. Scientific Reports, 14(1), 24632. https://doi.org/10.1038/s41598-024-76046-0

Vaccaro, D. T., & Sabella, L. D. (n.d.). Impact on Student learning: Monitoring student progress. Digital Commons @ University of South Florida. https://digitalcommons.usf.edu/jpr/vol3/iss1/5/

Lee, H., Park, S., Kim, E. H., Seo, J., Lim, H., & Lee, J. (2024). *I*nvestigating the effects of a real-time student monitoring interface on instructors' monitoring practices in online teaching. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (Paper 660). Association for Computing Machinery. https://doi.org/10.1145/3613904.3642845

Ratna, V., Khairnar, P., Bhardwaj, S., & Khatri, R. (2025). Securing academic social platforms: Implementing role-based access control (RBAC) in university-based digital systems. International Journal for Research Trends and Innovation, 10(5), Article IJRTI2505044. https://ijrti.org/papers/IJRTI2505044.pdf

Palve, S. S., & Palve, S. B. (2023). Attitude and perceptions of the faculty toward use of LMS in a tertiary medical college: An interventional study. Journal of education and health promotion, 12, 176. https://doi.org/10.4103/jehp.jehp_91_23

Tessitore, A. (2024, March 27). How Learning Management Systems help teachers enhance digital andragogy and drive innovation. OpenLMS. https://www.openlms.net/blog/education/learning-management-systems-enhance-digital-andragogy-drive-innovation/'

Dillon, R., & Tan, K.-L. (2024). Cybersecurity workforce landscape, education, and industry growth prospects in Southeast Asia. Journal of Tropical Futures. https://doi.org/10.1177/27538931231176903

Valdez, N. R., Rivera, M. V., & Pabico, J. P. (2015). Experiences in implementing an ICT-augmented reality as an immersive learning system for a Philippine HEI. Technological University of the Philippines. Retrieved from https://arxiv.org/abs/1601.06825

Aquino, M. F. M., & Noroña, M. I. (2021). Enhancing cyber security in the Philippine academe: A risk-based IT project assessment approach. Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management. Retrieved from https://www.ieomsociety.org/singapore2021/papers/878.pdf

Manalo, M. L. B., & Gallardo, R. D. (2024). Cybersecurity awareness and educational outcomes of Grade 4 learners. International Journal of Innovative Science and Research Technology, 9(4), 112–120. Retrieved from https://www.ijisrt.com/assets/upload/files/IJISRT24APR1261.pdf

Moldez, C., Crisanto, M. A., Cerdeña, M. G., Maranan, D. S., & Figueroa, R. (2024). Innovation in education: Developing and assessing gamification in the University of the

Philippines Open University Massive Open Online Courses. arXiv. https://doi.org/10.48550/arXiv.2409.03309

APPENDICES

Technical Background

Planning & Requirement Analysis Phase

Preliminary Investigation Answered Questionnaires.

Transcribed Interview, Observations.

Story Board.

Current Flow Chart / Process Flow.

Proposed Flow Chart / Process Flow.

Proposed Use Case Diagram

Specification & Design Phase

System Architecture / Module Specification

System Context Diagram

Data Flow Diagram

Data Dictionary

Hierarchical Input Process Output Model

Project Schedule

Hardware and Software Resources

Input/Output/Reports Screen Shots

Testing & Evaluation Instruments

Implementation Plan

User's Manual *(CD including Manuscript, System Package, Powerpoint, 5 pager)*

APPENDICES

Communication Letters & Forms

Request Letter

Pre-proposal Approval

Proposal Approval

Recommendation for Final Oral Defense

APPENDICES

5 Pager IMRAD Format

APPENDICES

Plagiarism Results

APPENDICES

Conference Presentation Narrative Report

APPENDICES

Certificate of Acceptance / MOA / MOU

APPENDICES

Curriculum Vitae