EKETE International Journal of Advanced Research
ISSN 3027-2513 (ONLINE)
ISSN 3027-169X (PRINT)

EKETE: International Journal of Advanced Research
Volume 3 Number 2, March 2025
url: https://journals.journalsplace.org/index.php/EKETE
Email: eketejournal@gmail.com

A WEB-BASED INTRUSION DETECTION SYSTEM FOR SOCIAL MEDIA FORUMS WITH INTRUDER IDENTIFICATION AND ACTIVITY LOGGING

Blessing Chinasa Mbah[1], S. C. Ikporo [2], Gift Adene[*3] and Christopher Tochukwu Mbah[4]

[1]Customary Court of Appeal, Enugu State
[2]Department of Computer Science, Ebonyi State University, Abakaliki, Ebonyi State, Nigeria.
[*3]Department of Computer Science, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State Nigeria
[4]Fashion Concept, Enugu State, Nigeria
[*]Corresponding Author e-mail: giftadene2016@gmail.com

Abstract

The Intrusion Detection Systems (IDSs) are systems designed to recognize malicious activities against computing resources and in turn protect against threats. The internet today is a great means of communication between users which ranges from social media to e-mails but hackers intruding to various users account have cause a lot of problems which ranges from inability of social media users to know those that attempt to login to their account, in ability of internet users to know the time, date of the particular user that tries to access or intrude to their account and also in ability to track and detect intruders details. These therefore led to the development of web based intrusion detection system for social network which will capture the date, time of the intruder or attacker and also block the intruders from gaining access to the system, easy retrieval of records of logs for quick decision making it also has detection and finally a central database for managing all records of attackers within a particular time. The methodology adopted to carry out this project work is Object Oriented Analysis and Design Methodology, this methodology is adopted because it is easy to understand and maintain, it provides re-usability, it reduces the development time and cost, and it improves the quality of the system due to program reuse.. This project work was developed using hypertext pre-processor (PHP5), JQUERY, and HTML5 scripting language and also cascading style sheet (CSS3) for the interface design, APACHE was used as the web server and MYSQLi for the database. After implementation this project the result showed that the research work was able to capture the intrusion attempt date and time and as well blocked the intruder from gaining access to the system. The system enhances security by detecting and logging intrusion attempts on social media forums, capturing the intruder's date, time, and IP address, and blocking unauthorized access while maintaining a centralized database for monitoring and decision-making.

Keywords: Intrusion Detection, Cyber Security, Social Media, Web Application, Software Engineering.

Introduction

An Intrusion Detection System (IDS) is a tool used to monitor networks and protect them from unauthorized access. With the rapid growth of internet-based technologies, new areas for computer networks have emerged, including fields such as business, finance, industry, security, and healthcare (Johnson & Lee, 2021). As the use of local area networks (LAN) and wide area networks (WAN) grows, these networks become increasingly attractive targets for abuse and vulnerabilities (Smith, 2020). Malicious users, or hackers, exploit internal systems to gather sensitive information and create vulnerabilities, such as software bugs, administrative oversights, and default system configurations (Williams, 2021). As the internet becomes more integrated into daily life, threats such as viruses and worms are becoming more common. Malicious users often use techniques like password cracking and detecting unencrypted text to compromise system security. Therefore, securing systems from these intrusions is crucial. Firewalls are a common security measure used to protect private networks from public networks. IDS are widely used in various fields, including network management, medical applications, credit card fraud detection, and insurance (Williams and Johnson, 2021). This work aims to address the limitations of existing intrusion detection systems by improving detection and logging mechanisms.

The internet facilitates communication via social media and emails, but unauthorized access by hackers poses security risks which ranges from the following:

1) Inability of social media users to know those that attempt to login to their account
2) Inability to track and detect intruder's details which include the date, time and the IP address used.
3) Inability to know the number of times the intruder access the account [i]trials to times

The aim of this work is to develop a real time intrusion detection system for social forum. The objectives are:

1) To create a module that would detect activities of attackers and also take records of all activities.
2) To create a module that will capture the date, time and also the IP-address of the intruders or attackers and also block the intruders from gaining access to the system.
3) To develop a centralize database management system that will manage all records of attackers' activities within a particular time.
4) To create a module that compares the activities and resources used by a particular user to the intrusion detection level that might be implemented for the user.

This study advances current IDS by integrating real-time intruder identification and activity logging, which not only detects unauthorized access attempts but also captures critical details such as date, time, and IP address while preventing further breaches. Additionally, it introduces a centralized database for managing attacker records and implements a comparative analysis module that assesses user activities against predefined intrusion detection levels, enhancing security monitoring and threat management beyond traditional IDS solutions.

Literature Review

Social media network platforms provide mechanisms that enhance the effectiveness of virtual socialization in the global village. It is a medium that enable families, friends, and associates to interact and communicate seamlessly irrespective of their locations, distances, and platforms. Online Social Networks (OSNs) are the connection and communication platform that promotes

the social interaction in the virtual space (Morris, 2021). Social media refers to websites and applications that are designed to allow people to share content quickly, efficiently, and in real-time (Adene *et al.,* 2021). While many people access social media through smart phone apps, this communication tool started with computers, and social media can refer to any internet communication tool that allows users to broadly share content and engage with the public (Hudson, 2020).

Musial and Kazienko (2016) identified 7 categories of social networks on the Internet to include: electronic mail services like Gmail, Yahoo mail, Microsoft outlook, Hotmail, etc; Instant messengers like WhatsApp, Twitter, Yahoo messenger, Instagram, Telegram, Snapchat, etc; Blogs platforms like Blogger, Tomblr, Wix, Linda etc; Social networking sites like Facebook, TikTok, Quora, LinkedIn, etc; Multimedia sharing systems like YouTube, Skype, Flikr, etc; Auction platforms like Jumia, Alibaba, Konga, OLX, etc; and Social search engines like Google, Yahoo, Safari, etc. All these platforms enable users to socialize and stay in touch with social reality in the virtual environment with varying functionalities. The pervasive nature of Information and Communication Technology (ICT) has greatly influenced every aspect of human activities; this has also influenced social media users to see the platform as a virtual home where they save their sensitive information on the database of these platforms. The growing reliance on the use of social media networks worldwide has resulted in great concern for information security. One of the factors popularizing the social media platforms is how they connect people worldwide to interact, share content and engage in discussions of mutual interest that know no geographical boundaries. Behind all these incredible gains, most traditional crimes now have digital equivalence enabling criminal minded elements and hackers to exploit social media platforms for many nefarious activities to harm others. As security administrators and policy makers develop detection tools to control these crimes, hackers' tactics and techniques are also constantly evolving. Hackers are cybercriminals that specializes in virtual terrorism that endangers the legitimate users of Social Media Network Platform (SMNP) in particular and the entire virtual community in general through various kinds of cyber-attacks (Timm, 2016).

These cybercrimes have significant negative impact on the social media platforms and the users in particular. Because of ease of accessibility, some of the social media users prefer to store their sensitive data on the network and when the account is hacked, this information could be used to swindle and defraud the user; also, the user's social contacts on the platform are at high risk of being defrauded by the hacker who could use their techniques by masquerading as the authorized user. High profile users like public and political leaders with private information that could tarnish their image if extracted can be used to threaten the user for ransom (Wang *et al.,* 2006).

Despite the tremendous impact in the development of different applications in intrusion detection, there exist some gaps that need to be solved. Wang *et al.,* (2006) developed an automatic tool for generating mobile agents for distributed IDS, in this design there is no means that detect activities of attackers and also take records of all activities.

Stolfo and Lee (2015) created a project that used intelligent, distributed Java agents and data mining to learn models of fraud and intrusive behaviors that can be shared between organizations, but this platform doesn't have the ability to keep records of logs for quick decision making and detection management.

Sebastian *et al.,* (2014) the authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to Event Gatherer‟ program. Event gatherer receives and convert alert messages in IDMEF standard

and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins, but despite this method the system does not have the ability to capture the date, time and also the IP-address of the intruders or attackers and also block the intruders from gaining access to the system.

Asaka, (1999) created an IDA which is a hierarchical architecture that relies on mobile agents to trace intruders among various hosts but this platform doesn't have a central database management system to manage all records of attackers' activities within a particular time and also compares the activities and resources used by a particular user to the intrusion detection level that might be implemented for the user.

The literature of this work highlights several previous Intrusion Detection System (IDS) models, each with distinct strengths and limitations. Table 1 is a comparative summary of these models and how the proposed system improves upon them.

Table 1: Comparative Analysis of Previous IDS Models and the Proposed System

S/N	Author(s)	Aim	Weakness/Limitations	Improvement in proposed System
1.	Asaka (1999)	Created a hierarchical IDS architecture based on mobile agents for tracing intruders.	Lacks a centralized database to manage attack records over time.	Incorporates a structured database system to track and analyze intruder activities for better decision-making.
2.	Wang *et al.*, (2006)	Developed an automatic tool for generating mobile agents for distributed IDS.	Lacks the ability to detect and log details of attackers' activities.	Introduces real-time detection with logging of attack attempts, including date, time, and IP address.
3.	Sebastian *et al.*, (2014)	Deployed IDS sensors across separate cloud layers, gathering and storing alerts in a central repository.	Fails to capture and block intruders' access attempts.	Blocks intruders from system access and provides real-time tracking of attack attempts.
4.	Stolfo and Lee (2015)	Used intelligent, distributed Java agents and data mining to learn fraud and intrusion patterns.	Lacks centralized logging for quick decision-making and detection management.	Implements a centralized database for monitoring and managing all intrusion records efficiently.

The proposed system enhances existing IDS solutions by integrating real-time detection, activity logging, automated blocking, and a centralized database for tracking intrusion attempts. Unlike previous models, it not only detects unauthorized access but also actively prevents intrusions and provides a structured record-keeping mechanism for improved threat management and user security awareness.

Materials and Methodology

The data used for this study were collected through both primary and secondary sources. The sample for primary data collection was selected from active social media users and administrators, with a focus on individuals who had experienced or managed intrusion attempts, ensuring relevance to the study. A convenience sampling approach was used due to accessibility and

willingness to participate, but efforts were made to include a diverse group to enhance the reliability of the findings. The research adopted quantitative methods for data collection and analysis, while Object Oriented Analysis and Design Methodology (OOADM) was used for software design and development. Methodology, as the word implies is described as a way of searching or solving the research problem. (Industrial Research Institute, 2015). In Methodology, researcher uses different criteria for solving/searching the given research problem. Different sources use different type of methods for solving the problem. For finding or exploring research questions, a researcher faces lot of problems that can be effectively resolved with using correct research methodology (Industrial Research Institute, 2015).

A thorough investigation of functional requirement of the present system and finding out whether the requirements and objective of the system are being achieved was made in order to obtain detailed facts about the application area to be re-designed. Direct observation, Interview, and examination of documents were carried out. The primary method used to detect unauthorized attempts to access social media accounts, such as Facebook or email accounts, involves sending a notification to the account owner's registered email address. This notification informs the user that someone has attempted to log into their account without proper authorization. In most cases, the message advises the account owner to take immediate action to secure their account by changing their password. The purpose of this approach is to alert users quickly and reduce the chances of the intruder successfully compromising the account. By requiring the user to change their password, this method ensures that any passwords potentially exposed to the intruder are rendered useless. It also reinforces security by encouraging the use of strong and unique passwords, which are harder for attackers to guess or exploit. This method relies on user awareness and action, as the security of the account depends on how promptly the owner responds to the alert. Another widely used method to detect and prevent unauthorized access to user accounts or systems involves the implementation of firewalls. A firewall serves as a protective barrier, acting as the first line of defence against cyber threats. It is designed to control and monitor incoming and outgoing network traffic based on predefined security rules or policies. Firewalls work by allowing or denying access to specific protocols, ports, or IP addresses based on predefined security rules, ensuring that only authorized network traffic is permitted while blocking potentially malicious activities. This is achieved by analysing the data packets traveling through the network and comparing them against a set of rules. If a packet does not meet the criteria defined by the policy, it is either blocked or redirected to prevent harm to the system.

In addition to these filtering functions, firewalls can "sniff" network packets, which means they inspect the content of data being transmitted at the boundary of the network. By doing so, firewalls can detect suspicious or unauthorized activities before they enter the system, ensuring that potential threats are mitigated early. Overall, firewalls are crucial for securing the entry points to a system, ensuring that only trusted and authorized traffic is allowed, while denying access to malicious or unknown sources. Combined with user notifications and other security measures, firewalls form an integral part of a multi-layered approach to protecting social media accounts, email platforms, and other systems from intrusion and malware attacks.

The flowchart in figure 1 describes the complete process of the existing system and how it works and functions in other to get the complete details of the existing system.

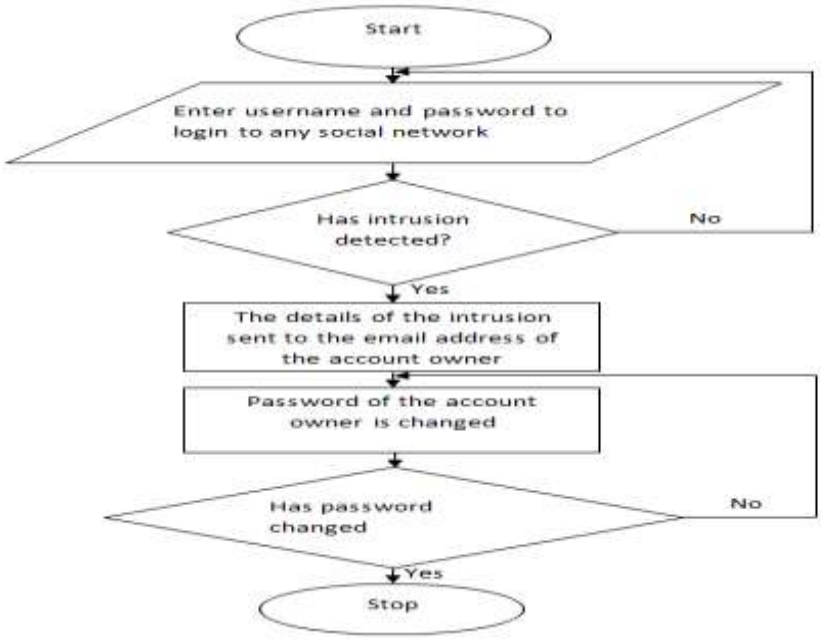

Figure 1: Flowchart of the Existing System

The existing system, while capable of detecting and preventing attacks, has notable weaknesses. It cannot inform social media users of login attempts, nor provide internet users with details such as time, date, and IP address of unauthorized access attempts. Additionally, it lacks the ability to track intruder details, monitor user activities, and instantly detect or protect against malicious threats on network resources. These limitations hinder comprehensive security and resource management.

The diagram in Figure 2 is the dataflow diagram of the New system which describes the complete flow of the system. The new system introduces two user roles: end users and administrators. End users must register to acquire login credentials, enabling them to access features like private and public chats. If an intrusion occurs, the system records details such as time, date, number of attempts, and intruder IP address, which are displayed on the user's dashboard upon successful login. Users can report threats to the administrator for further action, such as changing login credentials. The administrator monitors all user activities, views intrusion attempts, blocks intrusions, and communicates with users. The system tracks login attempts and user activities, providing accurate alerts for true and false intrusion events. Unlike platforms like Facebook and WhatsApp, this system captures the number of intrusion attempts and the IP address of intruders, enhancing security monitoring and threat management.

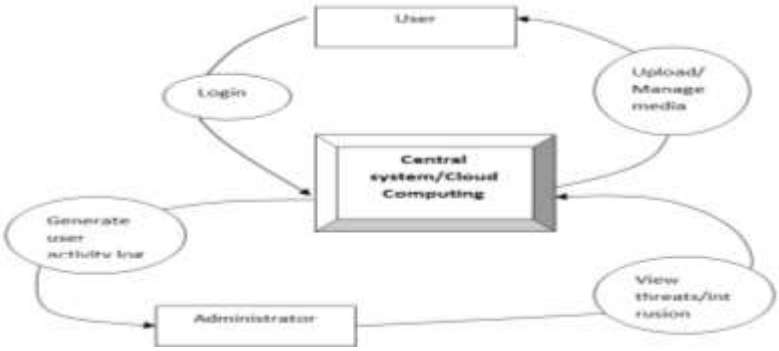

Figure 2: Dataflow Diagram of the New System

Implementation

After successful design of the system, the system was implemented and debugged for any syntax error. It followed the trend of testing, documentation and running in a xampp server environment. Any error identified was quickly corrected and the right syntax used.

After a careful analysis of the entire system, we chose to work with Adobe Dreamweaver CS5 as development environment and MySQL database as our development tools. The choice of Adobe CS5 was due to the fact that it has one of the best integrated development platforms that help in creating web applications at a very fast speed. It supports high level programming languages like PHP, JavaScript and other languages like HTML and CSS to provide a very user friendly environment to write and manage applications.

Our choice of MySQL database is due to the fact that it can be used to set up a query which, when applied to a database typically returns a set of records that matches your SQL (Structured Query Language) query, its popularity for the use in web based application, and it's widely used LAMP open source software stack. It is also used to handle large databases. The central database plays a vital role in the overall system, upon it information are kept and retrieved at intervals. The database structure and data format was designed to meet the specification of the system. It's a MySQL database that was designed with the SQL statement "create database" to store data that has been inputted into the system for storage. The name of the database that was created is intru_detect and it contains six tables which are charts table, login_details table, online_info table, trial_log table, update_status table, user_table.

Fig 3: Homepage Implementation

Figure 4: Main menu implementation

After successful deployment, the system was tested based on data presented. During the testing, the actual and expected results were compared to ensure they produced same result or if there is a difference, it should be slight and negligible. The result is shown in table 2.

Table 2: Comparison between expected and actual test results

TEST CONDUCTED	EXPECTED RESULT	ACTUAL RESULT
Login	The system checks for user login details to know if user has the right permission to access the system. If successfully validated the user is allowed to have access to the main page else an error message pops up which alerts the user of invalid login details	The system was able to check user login details to know if they have the right permission to access the system. On successfully validation it granted user access to the main page and for invalid login details an error message pops up that alerted the user of invalid login details
Update status	The user updates his/her status, by filling the text box, and upon clicking on the update button, it will be entered into the system and displayed on user main page	The user was able to update his/her status, by filling the text box, and upon clicking on the update button, it was entered into the system and displayed on user main page
Admin view logs of intrusion detected	Admin views all logs of possible threat and alerts users on possible actions, while taking necessary action	Admin was able to view all logs of possible threat and on clicking on the action button was able to suspend or reactivate user account.

Figure 5 is a line chart showing the performance comparison of the New System against previous IDS models in terms of:

- Detection Accuracy – Measures how well the system detects intrusions.
- False Positive Rate – Shows how often the system incorrectly flags legitimate users as intruders.
- Intrusion Response Time (ms) – Indicates the time taken to detect and block an intrusion.

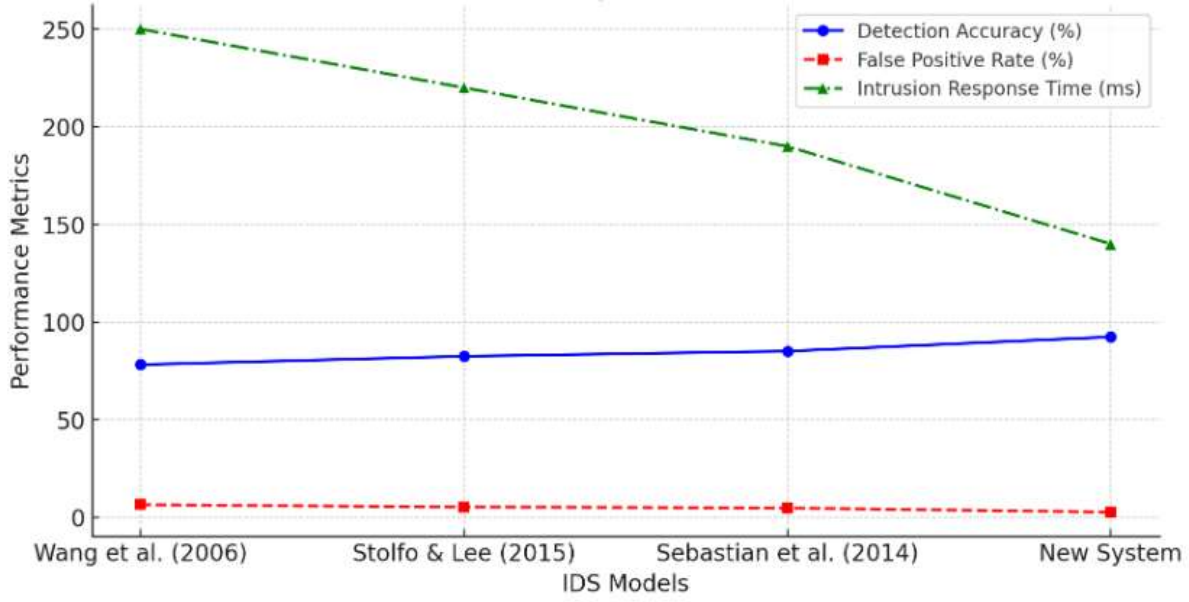

Fig 5: Performance Comparison of IDS models

Figure 5 illustrates the performance comparison of the New System against previous IDS models. Key takeaways include;

- Higher detection accuracy (blue line) shows improved intrusion detection capability.
- Lower false positive rate (red dashed line) indicates fewer incorrect flags on legitimate users.
- Reduced intrusion response time (green dotted line) highlights the system's faster threat mitigation.

This line graph reinforces the study's findings by showcasing how the New System outperforms existing IDS models in accuracy, efficiency, and reliability.

Conclusion

This work takes into cognizance effective monitoring in cloud computing technology, which provides advantages such as cost reduction and efficient resource management. The study successfully captures the date, time, and IP address of intruders or attackers while blocking unauthorized access to the system. Finally, a module was developed to compare user activities and resource usage against predefined intrusion detection levels, enhancing security measures.

Despite these advancements, the system has some limitations. It may generate false positives, incorrectly flagging legitimate users as intruders, which could lead to unnecessary access restrictions. Additionally, computational costs associated with real-time monitoring and data logging may affect system efficiency, especially under heavy traffic. The study also acknowledges the potential bias in intrusion detection rules, as predefined patterns might not cover all evolving cyber threats.

To address these limitations, future research should focus on reducing false positives through adaptive machine learning techniques, optimizing computational efficiency, and expanding intrusion detection criteria to accommodate dynamic and sophisticated cyberattacks. Additionally, future IDS models should explore energy-efficient (green computing), wireless-integrated (white computing), and cognitive (intelligent network-aware) systems for broader and more effective cybersecurity applications. Enhancing user authentication and security features across web applications will further strengthen protection against intrusions.

References

Adene, G., Ivo, A. S., Chikwendu, U. U., & Amaechi, E. M. (2021). Social media, a tool for increased visibility for engineering firms: Risks and benefits. *International Journal of Computer Trends and Technology, 69*(6), 61-65. https://doi.org/10.14445/22312803/IJCTT-V69I6P110

Asaka, K. (1999). An intrusion detection architecture (IDA) based on hierarchical architecture using mobile agents.

Hudson, M. (2020). What is social media? *The Balance SMB.* https://www.thebalancesmb.com/what-is-social-media-2890301

Industrial Research Institute Release. (2015). *Analysis report on the development prospect and investment strategic planning of China's big data industry from 2015 to 2020.* http://blog.sina.com.cn/s/blog_c4a726e70102wkvp.html

Johnson, A., & Lee, M. (2021). The evolution of intrusion detection systems in internet-based technologies. *Journal of Network Security, 34*(2), 45-60.

Morris, R. (2021). The role of intrusion detection systems in modern internet security. *Cybersecurity Journal, 15*(4), 212-225.

Musial, K., & Kazienko, P. (2016). Categorizing social networks on the internet: A comprehensive overview of online platforms.

Sebastian, R., Roschke, K., & Cheng, H. (2014). Deployment of intrusion detection system sensors on separate cloud layers for efficient event gathering and detection.

Smith, J. (2020). Vulnerabilities in business networks: A growing security concern. *International Journal of Cybersecurity, 29*(1), 88-97.

Stolfo, S., & Lee, W. (2015). Intelligent distributed Java agents and data mining for learning models of fraud and intrusive behaviors.

Timm, T. (2016). Evolving hacker tactics and their impact on social media network platforms and the virtual community.

Wang, Y., Gihan, V., Karl, N., & David, W. (2006). A network security monitor. In *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy* (pp. 296–304). IEEE Computer Society Press.

Wang, Y., Gihan, V., Karl, N., & David, W. (2006). An automatic tool for generating mobile agents for distributed intrusion detection systems (IDS).

Williams, B. (2021). Malicious attacks and defense mechanisms in network systems. *Computer Security and Networks Review, 25*(3), 158-174.

Williams, B., & Johnson, A. (2021). The evolution and advancements of intrusion detection systems. *Journal of Network Security, 39*(1), 112-125.