International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 11 | Nov 2022 www.irjet.net p-ISSN: 2395-0072

Cyber Intrusion Detection, Prevention, and Future IT Strategy

[1]Smrutirekha Panda

[1]Government College of Engineering, Keonjhar, Odisha India

***Abstract*:** The issue of guarding information and data movement has been there since the start of information exchange. Different approaches have been identified to protect and move such information safely. Due to the widespread use of modern technology, such as wireless communication, most organizations have become dependent on information technology. However, critical security and breaches are increasing in the contemporary world, creating the need for secure and safe information security systems. Intrusion detection and prevention are among the approaches used to improve the security and safety of information systems. The methodology used in the research is updated research on the exact condition of intrusion detection and prevention founded on risk analysis, an explanation of what intrusion detection and prevention are, and their primary functions. The findings are that security cases are rising; hence intrusion detection and prevention are highly required. Thus, further research should be conducted to advance the effectiveness and efficiency of intrusion uncovering and prevention.

Keywords: Risk management, Intrusion, Prevention, Detection, IT Strategy, KPI, IDSA

Introduction

In this modern era, an IT strategy supports business goals, competitive differentiation, and customer value. In fact, without a defined IT strategy, businesses cannot provide the level of service required by the company to achieve its goals. The modern world relies on Information Technology (IT) to perform most of its duties. Technology continues to advance to simplify some tasks and make the world a better place for human beings. According to Bashir and Chachoo (2014), the internet and e-commerce are more dominant than in the past. Individuals depend on information technology to conduct business, access news, and interact with each other. Moreover, vital information such as medical records, credit cards, and additional personal information is stored in computers for safety and easy retrieval. Businesses incorporate modern technology in their daily activities by creating a web page to aid their business performance. Researchers use computers to research and disseminate their findings (Sandhu et al., 2011, p.66). Thus, computers play a significant role in every individual's life. However, the integrity and availability of the systems should be highly protected from numerous threats associated with technological advancement. Amateur hackers, competing organizations, terrorists, and external authorities have the capacity and motive to conduct sophisticated computer attacks on computer systems. Thus, the information and communication security sector is vital for every individual's safety and economic well-being globally (Wattanapongsakorn et al., 2012). To present privacy breaches, security requires robust intrusion detection and prevention systems. This research paper aims to prove the current detailed condition of skill of intrusion detection and deterrence systems founded on risk analysis.

Background Information

Radoglou-Grammatikis and Sarigiannidis (2014) state that a better understanding of interference detection and prevention schemes will be possible by establishing the type of events they try to discover. An intrusion is a form of attack on data possessions where the instigator tries to get an entry into a system or interfere with ordinary operations (Karatas et al., 2014). Intrusions can also be the steps that try to exceed the security measures of computer systems. Thus, intrusions are any group of engagements that threaten the information and information systems' integrity, privacy, or availability. In this case, integrity refers to the data that has not been interfered with or damaged by unauthorized individuals in an unauthorized manner. Credibility implies that the information is not accessible or exposed to unauthorized parties, processes, or individuals. Availability means that a system with the needed data is accessible and can be used when required by authorized entities. In most cases, an intrusion results from an assailant retrieving the design from the internet or network or running an infected scheme or machine (see Fig 1). Moreover, intrusion also occurs when an attacker destroys third-party applications that control the information system (Patel et al., 2014). Attacks from external sources are called outside attacks. Attacks occurring

from within are called insider attacks, and they happen when unauthorized internal parties try to get access to specific information or misuse non-authorized access privileges.

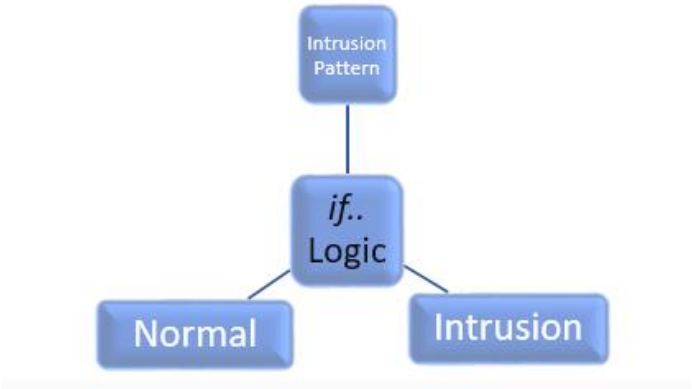

Fig 1. Conceptual Approach of Signature-based intrusion detection systems

According to Mudzingwa and Agrawal (2012), intrusion detection protects networks or computers from unauthorized access, action, or file alteration. Thus, an intrusion system can be a hardware or software device which systematizes the intrusion recognition procedure. An intrusion-finding organization can react to doubtful occurrences in one of the identified methods. First is by showing an alert to inform the security management, logging the situation, or calling an overseer (Mukhopadhyay et al., 2011, p.28). Intrusion prevention is interrupting the identified system attacks in actual time by ensuring they do not proceed to their aimed destinations. Intrusion prevention is vital against rejecting services, floods, and instinctual force attacks. Kuznetsov et al. (2012) define an intrusion prevention system as a hardware or software device with the abilities of an intrusion detection system that can try to prevent a likely attack from occurring. An intrusion prevention system can react to an identified threat by reconfiguring other security regulators in systems such as routers or firewalls to prevent future episodes (Ansari et al., 2022). The prevention can also occur when the system eliminates the questionable content of an attack in network circulation to sieve the intimidating packets. Finally, prevention can arise when the system reconfigures other security and confidentiality regulations in browser settings to evade future attacks.

Already et al. (2016) state that disabled prevention characteristics in the intrusion prevention items can work as intrusion detection systems. The prevention systems are viewed as an extension of the intrusion detection systems (Rajagopalan et al., 2017, p.2509). Although both systems assess network traffic looking for attacks, there are substantial differences. Intrusion detection and prevention systems identify malicious and unwanted traffic entirely and accurately, although they vary in how they reply to each other (Cheng et al., 2011, p.1011). The central role of intrusion detection is to warn of suspicious activity. In contrast, the prevention system's prominent role is active guarding to improve intrusion detection and other old security remedies, with the possibility of reacting in real time to evade or prevent malicious activities from occurring. Baykara and Das (2018) identify risk management as a vital aspect of a fruitful information technology security system and organizational KPI management. Thus, companies should employ risk management techniques to determine the security controls needed to mitigate risks satisfactorily (Patel 2017, p.92). To develop an effective intrusion detection and prevention system, appropriate requirements apprehension based on risk management is crucial.

Importance of risk management

Technology has been gradually changing through networking, bringing people together no matter the continent. Therefore, communication systems and all computers are expected to be protected; intrusion detection systems are created to monitor any network activities in the machine and those that are outgoing (Chakir et al., 2017). The intrusion detection system can identify any signs of threat or suspicious activities that might compromise the system and raise the alarm to the responsible team. The system is being protected from various attacks, such as digital forensic and fault tolerance functions, accidents, and abuse of security breaches (Al janabi, 2017; Dash & Sharma, 2022). System vital information is protected so that

i0t can be reliable, available, and trusted by many. The computer and system information are expected to be safe and identifiable. Risk is the calculation of all adverse impacts that might happen to computer information systems and the probability that the information in the system is vulnerable to cybercrime (Dash & Ansari, 2022).

As stated by (Patel et al.,2017,p.92), risk management, through its significant roles of identifying, assessing risk, and taking it to another stage, can reduce those risks and vulnerabilities to a minimum level that can be comfortable to everybody else in the company, risk management is run by the information technology managers trying to balance operational and economic costs by monitoring and evaluating some of the threats and setting traps to intruders to cut short their plans by introducing some antivirus software. Information technology managers can detect attacks from various sources, such as distribution denial and port scanning attacks which enable intrusion and detection to produce a shield against unauthorized individuals getting into the system of any company (Al 2017, p.51). Risk management can provide the users with a time or mechanism to block the intruders for time t, enabling them to buy time as they are preparing to sell those gaps and provide specific information to the various departments that are likely to be attacked (Khraisat & Alazab, 2021) indication. It also acts as a security barrier that can detect and disallow the attacks before they think to penetrate the inner circle (see Fig 2). Risk management introduces the idea of security layers that become more difficult for attackers to access critical information targeted by intruders.

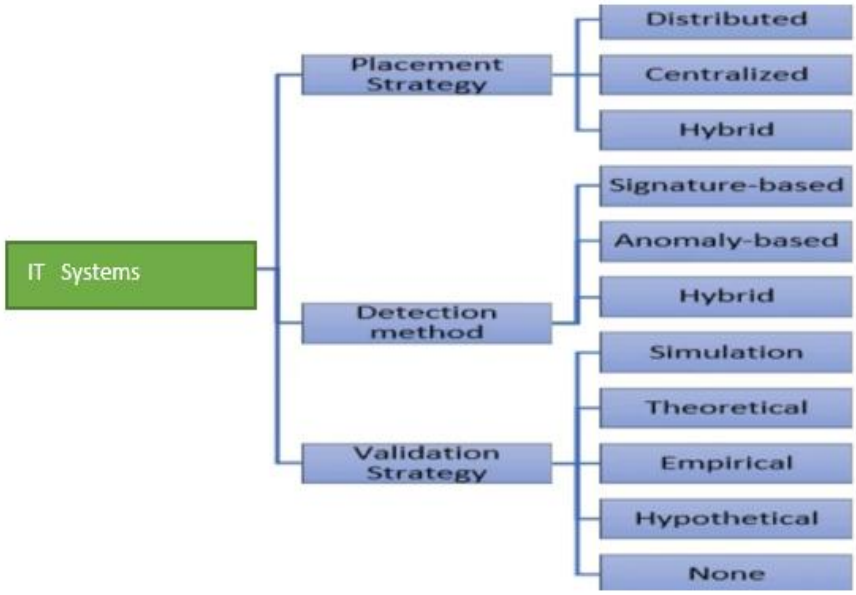

Fig 2. Classification of Intrusion Detection System Architecture (IDSA)

Risk management plays a vital role in a successful information technology program. It allows the organization to set realistic goals at the right time without obstacles. When the information and documents of the company are stored in a safe and protected system, the confidentiality and trust of the client's i9s are boosted to a higher level, enabling the organization to proliferate (Zarpelao et al.,2017, p.25). The individual mandated to operate and manage the information technology system in an organization should not take the risk management process lightly technical function but as a vital critical backbone of the organization. The risk management process has its components, such as the risk-based strategies that allow for identifying, mitigating, and understanding the threats associated with the system and the use of information. For the organization to feel more secure, it must borrow the ideal of risk-based strategies. This enables the organization to be protected from severe and sophisticated risks to information systems. An organization must provide the facilities to ensure that data is safe and trusted. Risk management ensures that information is available and confidential (Liu & Zang 2016; Ansari et al., 2022a) be constantly updated. Risk management allows information technology experts to compare all activities against a pool of collected attack signatures.

Intrusion Detection and Prevention Systems

Liao et al. (2013) define intrusion detection as observing the occurrences happening in a computer structure or a system and examining them for emblems of probable affairs. The discussed events are usually defilements or future threats of destruction of computer safety guidelines, acceptable strategies, or standard security practices (Modi et al., 2013, p.42). An intrusion detection service is a software request or a device that controls information systems or networks from dangerous activities or policy defilements and replies to the malicious activity by cautioning the system overseer by either creating an alert, logging the action, or contacting the manager (Sharafaldin et al., 2018; Ansari, 2022).

Intrusion prevention is when active intrusion detection tries to stop or avert an identified possible threat before bringing any harm to the system. An invasion prevention scheme is a software or device with all the features and abilities of an intrusion detection system, but it can prevent a potential threat (Schönefeld & Möller 2012, p.31). The intrusion prevention systems are planned and established for various active protection to make intrusion detection and traditional security remedies better and more effective. Research shows that an intrusion prevention system is the incoming security technological level due to its ability to offer security at different system levels ranging from the functioning kernel to network data packages (Alves et al., 2018). Prevention systems are designed to guard information systems from illegal access, destruction, or disruption (see Fig 3). In contrast, intrusion detection systems identify a possible attack for the prevention system to stop or avert the attack (Conte et al., 2020, p.1). Another difference between intrusion detection and intrusion prevention system is that intrusion prevention systems can prevent known intrusion sensed signatures, apart from the unrecognized attacks coming from the database attack of generic conducts.

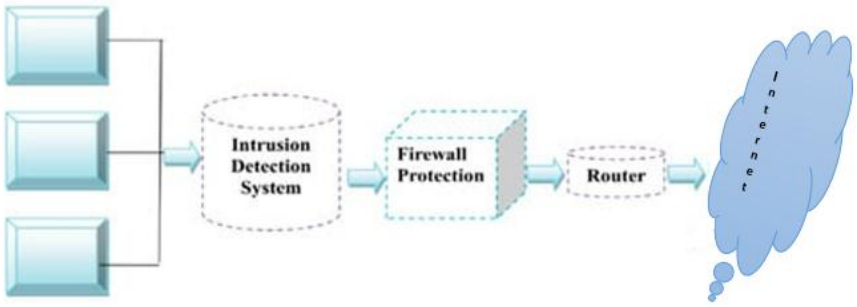

Fig 3. Intrusion Detection Management System

The current invasion detection and prevention schemes are encompassed two predominantly varying approaches, the network-based model and the host-based model. In the recent past, a new direction, application-based, was added to intrusion detection, which is an improvement of the host-based approach (Das and Sarkar 2014, p.2266). Thus, the workstations and servers are guarded by the host-based invasion detection and prevention system via a safe and regulated software communication media between the system's applications and the functioning system kernel. According to Biswas and Roy (2019), the software is pre-configured to identify the protection guidelines founded on intrusion and attack autographs. The host-based intrusion detection and prevention system will clasp distrustful events within the system. The predetermined policies will either stop the event from happening or allow the event to proceed. The host-based intrusion detection and prevention systems oversee events such as application or data requirements, network link trials, and read or write tests (Alhello et al., 2017). The main disadvantage of the host-based invasion detection and anticipation systems approach is that with the necessarily tight integration with the host functioning system, future functioning system improvement could result in some issues.

Mazzini et al. (2019) define network-based invasion detection and prevention systems as software or a focused hardware structure that links directly to a network portion and guards every system connected to the same or downstream system portions. Network intrusion devices and prevention systems expedients are used according to the guarded network portion. All the information between the protected and fundamental parts of the system must go through the network intrusion detection and prevention system device (Yousufi et al., 2017). As the circulation goes via the device, it is examined to

determine if there is any possibility of an attack. If there is any possible attack, the network invasion detection and prevention system is abandoned or prevents the offending data from going through the system to the targeted victim, avoiding the attack. The network-based intrusion detection and prevention systems will interrupt all network traffic and observe it for distrustful events and activities, preventing the demand or passing it. However, it should be viewed as genuine traffic. The most attractive feature of network-based invasion detection and prevention schemes is that if the system recognizes a felonious information packet, it can rewrite the packet for the attack attempt to be unsuccessful (Nayyar et al., 2020, p.136). In this case, an organization can identify the event to collect evidence against the attacker without the attacker's knowledge. Despite whether the user operates the host-based, network-based, or application-based level, every invasion detection and prevention system employs one of the two detection approaches: anomaly-based.

An anomaly detection technique is developed to disclose the strange features that diverge from the identified normal behavior. Happening the other arrow, the invasion discovery and prevention systems form a foundation of regular usage patterns. Any activity significantly deviates from the system becomes flagged as a potential intrusion (Jafarian et al., 2021, p. 1235). An anomaly intrusion can be different, but an individual should realize that if any event occurs, more or less than the two typical deviations from the statistical behavior would create an alarm (Hu et al., 2017, p.10). For example, if a user logs on to a device more than eight times a day as an alternative to the regular one to two times a day, there would be an alarm. Additionally, if an office computer is accessed at 3;00 AM, there would be an alarm because these are not regular business hours. According to Sonmez et al. (2018), anomaly detection can examine user behavior by analyzing the programs accessed daily. For instance, if anomaly detection finds that a user in the information technology department abruptly starts accessing marketing programs, the system will raise the alarm or inform the management because it might be a possible intrusion.

Jose et al. (2018), the main advantage of anomaly detection techniques is that they effectively capture formerly unidentified threats. In most cases, the system must understand normal behavior in the first stage of using an anomaly-based detection model. If the regulated system performs, it will be assumed normal behavior. There should be no attack in the regulated system in the learning phase to ensure the intrusion detection and prevention system does not study to overlook attacks. The learning phase can be dealt with in numerous ways, such as machine wisdom or creating statistical behavioral outlines. The system encounters attacks in the following implementation stage (Behniafar et al., 2018, p.79). Thus, the intrusion discovery and prevention systems observe the events in the regulated system and relate them to the studied standard behavior patterns. If they do not align, suspicion is raised, and if the fear exceeds a specific level, the system increases the alarm (Ding et al., 2019, p.106458). The primary significance of the anomaly-based detection method is that it does need past awareness of invasion; hence it can capture novel intrusions without external interventions. However, the technique has a drawback because it might fail to explain an attack, and it can issue a false positive rate.

Unauthorized conduct is usually detected by the system's abuse and is mainly referred to as signature detection. Nevertheless, this detection method employs identified patterns of unauthorized behavior to forecast and identify succeeding similar efforts. Signatures are the exact configurations (Azeez et al., 2020, p.685). Three unsuccessful logins are examples of a signature in host-based invasion detection and prevention system. A signature in intrusion detection and prevention systems can be easy, like an exact arrangement matching a net package section. For example, package content signatures or caption content signatures can symbolize illegal occurrences. The signature action might not represent the absolute attempted illegal admission because it can be an unintentional error (Masdari & Khezri 2020). However, it is vital to take every system alert with much seriousness. Specific alarms, replies, or warnings should be directed to the relevant authorities depending on the strength and severity of the signature.

Łukasiak and Rosiński (2017) state that the idea underlying exploitation detection systems are that there are methods to present attacks in pattern or signature form for the differences of comparable attacks to be identified. Therefore, the schemes are like virus detection structures because they can recognize numerous specified attack arrangements. However, the systems cannot be significantly employed in unknown attack models. It is vital to note that the anomaly detection method attempts to identify known lousy conduct. The primary matters in misapplication detection systems are designing a signature that includes every potential difference of the relevant attack and creating signatures that align with non-intrusive events. The benefit of the misappropriation detection system is that it can efficiently and effectively identify situations of known attacks (Kumari & Sharma 2018, p.38). The primary drawback of the misuse detection scheme is that it cannot identify recently

discovered attacks. Thus, signature databases should be updated regularly, and intrusion detection systems should relate and align the events with massive collections of attack signatures.

Why be serious about Intrusion

All organizations are putting more effort into security, especially those using information systems, and are required to take security matters seriously to boost confidentiality, safety, and trust among the users. Therefore, some companies are developing new skills that allow them to create new rules that can provide security solutions to threats that might arise from external or internal attacks. In any organization, Information security should handle information technology experts who can control and filter any information damage that might arise from internal threats. (Attie et al., 2018). Moreover, the organization drafts network security-based, which protects the information systems by detecting attacks and providing clear guidelines to strengthen defense and keep information more secure. Some companies have tried to adopt various ways to keep information systems safe, such as thy cryptographic (Dahiya & Srivastava 2018, p.253). Cryptography faces some challenges, for instance, the users may forget their passwords or the password might be cracked, or all cryptosystems are lost, and the information is left in the hands of attackers and this coalition between insiders in the company and the outsiders.

Through the advance in technology, for instance, from 2010, users got a short notification via emails from various companies when the database was hacked. Therefore, all the users can log into their account from their comfort zone to alter the password immediately to reduce more damage. Most hackers' details target credit card information, passwords, and email addresses (Yu et al.,2018, p.158). Recent statistical research indicated that with the advancement in technology and communications, the insecurity of the database is becoming more exposed to attackers and becoming very complicated now. You must change the routes so that it does not get familiar to the attackers. The rise of attackers encourages companies to be more focused, take holistic security measures, and ensure that information security programs are kept healthy (Kumari et al.,2017, p.824). There is a need for the organization to improve the technology because the old methods cannot be used to identify the new intruders that breach and violate the database and prevent interference with the data and maintain the privacy of the organization, and in any case, be able to respond to any threats and provide the solution to the problem immediately (Shreenivas & Voigt 2017). Therefore, the system needs to be updated to acquire more intelligent programming techniques and knowledge-based strategies to withstand all the threats that can harm the information system. The information technology experts need to build formidable efforts systems that ensure no one can access the company's information without their knowledge.

Here are some incidents that happened in the United States of America during the year. In January, an employee from the human resource department of the library of congress stole information from the library database, which contained information about all the employees in the company, and was charged with wire fraud. The accessed then used the acquired knowledge to pass to various links, including his relative specialized in opening accounts. The figures indicated that they get a lot of money from hacked accounts (Sinh et al., 2019). The accused individuals then passed the information to those who were traced to be in Ukraine. The breach was estimated to [have affected so many people, with around one hundred and sixty thousand of the bank's users exposed to the Ukrainian attack site.

In February, another suspect was arrested, which provided critical information to the law enforcement agency, and a computer file with Kaisers' permanent data was seized. Though the individual was not an employee of Kaiser, Kaiser Permanente had to notify all the northern Californian staff about what happened for their personal information to be released. It concerned the breach of the security system in the department. In the same month, the database of the USA Kaspersky was compromised by an unidentified hacker who accessed essential information such as the security numbers of the staff of Kaspersky (Rios et al., 2020; Dash, 2021). At the University of Alabama, some computers were stolen, containing personal information such as lab results, names, and addresses of those who had to undergo lab tests.

Some of the customer's credit numbers were stolen in March 2009 from Symantec Company. And the company had to send frequent letters to notify its customers about the security breach of some of its members in the United Kingdom and Canada. In the month of April, one of the former employees in the New York state tax department stole many identities belonging to taxpayers and used them to create more accounts which were used for fraudulent activities by contacting individual personal data as by (Kasongo & Sun et al.,2020, p.98). And one of the former information technology experts in the

bank was arrested. His documents were social security numbers, names of various employees and customers, and driving license, which was fake. In August, several hackers invaded the University of Massachusetts server and managed to access a computer server, hijack all graduates' information, and defraud them (Bhavani et al.,2020, p.637). In September, it was a blow to the Keystroke logging, the hackers stole the critical components used by the for-banking purpose, and they further transferred a tremendous amount of money into the company account. Research indicates that hackers access bank details through women's data in UNC-Chapel Hill. They were about two hundred and thirty-six thousand, and some other information that was interfered with included the mammography Registry.

In the month of October 2009, the hackers were able to access United States Army special forces. They got away with necessary credentials, including names, home addresses, and cell phone numbers. In the same month, a computer technician in Mellon corps company was arrested and charged because he had stolen many identities from various banks and used them to defraud charitable groups .and. In November, multiple customers raised suspicious alarms to the bank of Hancock bank customer in California about their ATM withdrawals (Dominique & ma, 2018). In December, computers were breached. Many documents were stolen in the Lincoln campus of the Department of Education and human sciences, including other graduation lists. When the investigation was done, experts indicated that computers were not properly secured, which allowed more access s to various individuals from external outsiders. During the same period, Pennsylvania State University acknowledged the breach of security on the campus and the letters sent to multiple students responsible for fraudulent activities on campus. The college had to set records straight for those students to those involved in malicious intrusions. Therefore, any strange behaviors must be detected, and the alarm must be raised to prevent significant damage from occurring.

Conclusion and Recommendation

The modern interrelated computer connection is a hazardous reality because it has numerous individuals with much time to spend against the most solid security measures. Such individuals can be defeated by identifying when they are likely to attack to prevent their attempts. Developing appropriate strategies is the key and choosing the proper intrusion detection and prevention system is vital to ensure that an organization's network and systems are safe and secure. While security cases continue to increase, intrusion detection and prevention systems and enabling tools are crucial to improving security. The intelligent intrusion detection and prevention system and the instruments should integrate several philosophical approaches from the topics of autonomic computing, machine learning, data mining, and artificial intelligence to aid them in identifying what approves an intrusion against a regular activity. This will be enabled by developing a knowledge foundation that improves when novel ideas or knowledge are discovered. Intrusion detection and prevention systems are an inexperienced research area. Nevertheless, the field is gaining substantial importance in the modern computing environment. The integration of facts such as the emotional internet development, the enormous financial potentials in electronic trade, and the absence of secure systems make it a vital research and improvement area.

Future research and development patterns appear to be meeting towards an approach founded on multi-agent invasion detection and prevention systems based on and controlled by autonomic computing artificial intelligence and data mining to support anomaly intrusion detection. The autonomic computing features such as self-configuration, self-healing, self-preservation, and self-optimization should be improved to comprise self-prevention and self-detection. The outcomes of the techniques will help research to differentiate malicious activities from regular non-attack events. Thus, the intrusion detection and prevention systems will be an innovative and challenging section of the security administration scheme with a rich but shortened alarm supervision and demonstration of security defilement activities for easy human consumption.

References

Al Quhtani, M., 2017. Data Mining Usage in Corporate Information Security: Intrusion Detection Applications. *Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy*, *8*(1), pp.51-59

Alhello, Z.A., Abdul, A. and Kaur, H., 2017. On Applicability of Neural Network in Intrusion Detection and Prevention. *International Journal of Advanced Research in Computer Science*, *8*(7).

Al-Janabi, S., 2017, November. Pragmatic miner to risk analysis for intrusion detection (PMRA-ID). In *International conference on soft computing in data science* (pp. 263-277). Springer, Singapore.

Alneyadi, S., Sithirasenan, E. and Muthukkumarasamy, V., 2016. A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, *62*, pp.137-152.

Alves, T., Das, R. and Morris, T., 2018. Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *IEEE Embedded Systems Letters*, *10*(3), pp.99-102.

Ansari, M., Dash, B., Sharma, P., & Yathiraju, N., 2022a. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering, 11(9), 81–90. https://doi.org/10.17148/IJARCCE.2022.11912

Ansari, M.F., 2022. A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs. International Journal of Smart Sensor and Adhoc Network, 3(3).

Ansari, M.F., Sharma, P.K. and Dash, B., 2022. Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. Prevention. https://doi.org/10.47893/ijssan.2022.1221

Attia, M., Senouci, S.M., Sedjelmaci, H., Aglzim, E.H. and Chrenko, D., 2018. An efficient intrusion detection system against cyber-physical attacks in the smart grid. *Computers & Electrical Engineering*, *68*, pp.499-512.

Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., Van der Vyver, C. and Ahuja, R., 2020. Intrusion detection and prevention systems: an updated review. *Data management, analytics and innovation*, pp.685-696.

Bashir, U. and Chachoo, M., 2014, March. Intrusion detection and prevention system: Challenges & opportunities. In *2014 International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 806-809). IEEE.

Baykara, M. and Das, R., 2018. A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications*, *41*, pp.103-116.

Behniafar, M., Nowroozi, A.R. and Shahriari, H.R., 2018. A survey of anomaly detection approaches in the internet of things. *The ISC International Journal of Information Security*, *10*(2), pp.79-92.

Bhavani, T.T., Rao, M.K. and Reddy, A.M., 2020. Network intrusion detection system using random forest and decision tree machine learning techniques. In *First international conference on sustainable technologies for computational intelligence* (pp. 637-643). Springer, Singapore.

Biswas, S. and Roy, A., 2019, June. An intrusion detection system-based secured electronic service delivery model. In *2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1316-1321). IEEE.

Chakir, E.M., Moughit, M. and Khamlichi, Y.I., 2017, May. A real-time risk assessment model for intrusion detection systems. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

Cheng, T.H., Lin, Y.D., Lai, Y.C. and Lin, P.C., 2011. Evasion techniques: Sneaking through your intrusion detection/prevention systems. *IEEE Communications Surveys & Tutorials*, *14*(4), pp.1011-1020.

Conte, K.P., Ryder, T.J., Hopkins, L., Gomez, M. and Riley, T., 2020. Committed, ambivalent, concealed, or distanced: community organisations' perceptions of their role in local prevention systems. *Critical Public Health*, pp.1-11.

Dahiya, P. and Srivastava, D.K., 2018. Network intrusion detection in big dataset using spark. *Procedia computer science*, *132*, pp.253-262.

Das, N. and Sarkar, T., 2014. Survey on host and network-based intrusion detection system. *International Journal of Advanced Networking and Applications*, *6*(2), p.2266.

Dash, B., & Ansari, M. F., 2022. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

Dash, B., & Sharma, P., 2022. Role of Artificial Intelligence in Smart Cities for Information Gathering and Dissemination (A Review). Academic Journal of Research and Scientific Publishing| Vol, 4(39).

Dash, B., 2021. A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).

Ding, N., Ma, H., Gao, H., Ma, Y. and Tan, G., 2019. Real-time anomaly detection based on long short-term memory and Gaussian Mixture Model. *Computers & Electrical Engineering*, *79*, p.106458.

Dominique, N. and Ma, Z., 2018, December. Enhancing network intrusion detection system method (nids) using mutual information (rf-cife). In *International Conference on Security with Intelligent Computing and Big-data Services* (pp. 329-342). Springer, Cham.

Hu, Z., Gnatyuk, S., Koval, O., Gnatyuk, V. and Bondarovets, S., 2017. Anomaly detection system in secure cloud computing environment. *International Journal of Computer Network and Information Security*, *9*(4), p.10.

Jafarian, T., Masdari, M., Ghaffari, A. and Majidzadeh, K., 2021. A survey and classification of the security anomaly detection mechanisms in software defined networks. *Cluster Computing*, *24*(2), pp.1235-1253.

Jose, S., Malathi, D., Reddy, B. and Jayaseeli, D., 2018, April. A survey on anomaly based host intrusion detection system. In *Journal of Physics: Conference Series* (Vol. 1000, No. 1, p. 012049). IOP Publishing.

Karatas, G., Demir, O. and Sahingoz, O.K., 2018, December. Deep learning in intrusion detection systems. In *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)* (pp. 113-116). IEEE.

Kasongo, S.M. and Sun, Y., 2020. A deep long short-term memory based classifier for wireless intrusion detection system. *ICT Express*, *6*(2), pp.98-103.

Khraisat, A., & Alazab, A., 2021. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1), 1-27.

Kumari, R. and Sharma, K., 2018. Cross-layer based intrusion detection and prevention for network. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 38-56). IGI Global.

Kumari, U. and Soni, U., 2017, October. A review of intrusion detection using anomaly based detection. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 824-826). IEEE.

Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A. and Berezovsky, A., 2015. The statistical analysis of a network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering*, *74*(1).

Liao, H.J., Lin, C.H.R., Lin, Y.C. and Tung, K.Y., 2013. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), pp.16-24.

Liu, Y. and Zhang, X., 2016, August. Intrusion detection based on IDBM. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 173-177). IEEE.

Łukasiak, J. and Rosiński, A., 2017. Analysis of exploitation process in the aspect of readiness of electronic protection systems. *Diagnostyka*, *18*.

Masdari, M. and Khezri, H., 2020. A survey and taxonomy of the fuzzy signature-based intrusion detection systems. *Applied Soft Computing*, *92*, p.106301.

Mazini, M., Shirazi, B. and Mahdavi, I., 2019. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University-Computer and Information Sciences*, *31*(4), pp.541-553.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. *Journal of network and computer applications*, *36*(1), pp.42-57.

Mudzingwa, D. and Agrawal, R., 2012, March. A study of methodologies used in intrusion detection and prevention systems (IDPs). In *2012 Proceedings of IEEE Southeastcon* (pp. 1-6). IEEE.

Mukhopadhyay, I., Chakraborty, M. and Chakrabarti, S., 2011. A comparative study of related technologies of intrusion detection & prevention systems. *Journal of Information Security*, *2*(01), p.28.

Nayyar, S., Arora, S. and Singh, M., 2020, July. Recurrent Neural Network-Based Intrusion Detection System. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0136-0140). IEEE.

Patel, A., Alhussian, H., Pedersen, J.M., Bounabat, B., Júnior, J.C. and Katsikas, S., 2017. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. *Computers & Security*, *64*, pp.92-109.

Patel, A., Alhussian, H., Pedersen, J.M., Bounabat, B., Júnior, J.C. and Katsikas, S., 2017. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. *Computers & Security*, *64*, pp.92-109.

Patel, A., Qassim, Q., Shukor, Z., Nogueira, J., Júnior, J., Wills, C. and Federal, P., 2011. Autonomic agent-based self-managed intrusion detection and prevention system. In *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)* (pp. 223-234).

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Karypidis, P.A. and Sarigiannidis, A., 2020, August. Diderot: an intrusion detection and prevention system for dnp3-based SCADA systems. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-8).

Rajagopalan, R., Litvan, I. and Jung, T.P., 2017. Fall prediction and prevention systems: recent trends, challenges, and future research directions. *Sensors*, *17*(11), p.2509.

Rios, A.L.G., Li, Z., Bekshentayeva, K. and Trajković, L., 2020, October. Detection of denial of service attacks in communication networks. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)* (pp. 1-5). IEEE.

Sandhu, U.A., Haider, S., Naseer, S. and Ateeb, O.U., 2011. A survey of intrusion detection & prevention techniques. In *2011 International Conference on Information Communication and Management, IPCSIT* (Vol. 16, pp. 66-71).

Schönefeld, J. and Möller, D.P.F., 2012. Runway incursion prevention systems: A review of runway incursion avoidance and alerting system approaches. *Progress in Aerospace Sciences*, *51*, pp.31-49.

Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A., 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, *1*, pp.108-116.

Sharma, P., Dash, B., & Ansari, M. F., 2022. Anti-phishing Techniques – A Review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728

Shreenivas, D., Raza, S. and Voigt, T., 2017, April. Intrusion detection in the RPL-connected 6LoWPAN networks. In *Proceedings of the 3rd ACM international workshop on IoT privacy, trust, and security* (pp. 31-38).

Singh Panwar, S., Raiwani, Y.P. and Panwar, L.S., 2019, March. Evaluation of network intrusion detection with features selection and machine learning algorithms on CICIDS-2017 dataset. In *International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India*.

Sönmez, F., Zontul, M., Kaynar, O. and Tutar, H., 2018. Anomaly detection using data mining methods in it systems: a decision support application. *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *22*(4), pp.1109-1123.

Wattanapongsakorn, N., Srakaew, S., Wonghirunsombat, E., Sribavonmongkol, C., Junhom, T., Jongsubsook, P. and Charnsripinyo, C., 2012, June. A practical network-based intrusion detection and prevention system. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 209-214). IEEE.

Yousufi, R.M., Lalwani, P. and Potdar, M.B., 2017, March. A network-based intrusion detection and prevention system with multi-mode counteractions. In *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-6). IEEE.

Yu, J., Hao, R., Xia, H., Zhang, H., Cheng, X. and Kong, F., 2018. Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction. *Information Sciences*, *442*, pp.158-172.

Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C., 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, pp.25-37

Author Biography

Smrutirekha Panda is a final year Electrical engineering student at Government Engineering College, Keonjar, Odisha, India. Her research interests are Artificial Intelligence, Cloud Computing, Information Systems, Big Data, and the Internet of Things.