Human Interaction and Emerging Technologies (IHIET-AI 2025), Vol. 161, 2025, 322–332
https://doi.org/10.54941/ahfe1005924

Security in Information Systems With Artificial Intelligence: Development of AI-Based Threat Detection Systems to Protect Information Integrity

Nelson Salgado Reyes

Pontifical Catholic University of Ecuador, Faculty of Information Systems Engineering, Quito, 12 de Octubre Avenue 1076 and Vicente Ramón Roca, Ecuador

ABSTRACT

This investigation aims to evaluate the progress in artificial intelligence (AI) threat detection systems, to strengthen information-system security, which has been achieved by guaranteeing integrity, confidentiality, and availability of information. The results further highlight the use of AI to proactively detect and mitigate unseen attacks before they cause any real damage. Using a qualitative methodology as an investigatory framework, this research reflects an interpretative fine-tooth analysis of the literature to provide evaluation of how AI has been used in prevention and containment. The study also discusses different AI methodologies like machine learning, deep learning, neural networks and how they provide a boost in threat detection. A literature review provides a critical examination and analysis of former studies, highlighting patterns, trends, and new methodologies that underscore the ongoing maturation and intricacy of Internet related threats balancing cybercrime AI countermeasures. High-level takeaways from the results Here are some of the chief findings about how AI can protect your network: General adaptation: When attacking patterns shift away from traditional deterministic rules detection, cyberthreats remain hidden from the human eye. The report also explores the use and implementation of AI along with other security systems including encryption and blockchain to establish multiple defence layers. The integration noticeably enhances the resilience of information systems, making them stronger against APTs and Zero-day attacks. It also focuses attention on the wealth of qualitative data with which to explore more nuanced aspects of information security. This complete view helps to bring further clarity to both the issues and potential of AI-driven security solutions. These results underscore the importance of addressing how to use AI as a critical component in building successful digital security information protection strategies and should argue for its wider implementation throughout industries. The research concludes by recommending further exploration of AI's role in predictive analytics and automated incident response, areas where its potential remains underutilized.

Keywords: Computer security, Artificial intelligence, Threat detection, Information systems, and Confidentiality

INTRODUCTION

One of the most important intersections that are making security in information systems and artificial intelligence one of the critical areas in our digital age. With this scenario, it is now mandatory to create security actions that use artificial intelligence for the detection of threats and maintain information integrity and confidentiality. This will be a proactive approach to the increasing sophistication of cyber threat actors that are present in the threat landscape. My research in this field focuses on addressing the complexity of cyber threats by utilizing state-of-the-art technologies. This research will specifically delve into the linkage between artificial intelligence and cyber security with the view of looking at some case studies and devising potential tactics to beef up our information systems.

The very first one is the vulnerability analysis using the open-source intelligence tools (OSINT) that was covered by Cusme & Zambrano (2022); In this way, it helps in recognizing potential security breaches and stay a step ahead by predicting upcoming breaches. This we complement with the review of security strategies in the network infrastructure, and addressing both common place issues and solutions provided by Lara (2023) research published on VICTEC Scientific and Technological Journal.

In the context of Ecuador, the following sections will present a wider discussion taking as reference: The work of Mosquera-Chere (2021), linking artificial intelligence with cybersecurity providing a relevant regional perspective. On the other hand, it will also refer to the programming of artificial intelligence schemes for the detection of cyberbullying as Cevallos (2021) has suggested. It underscores the significance of AI in safety of the vulnerable users online.

In another scenario applied to gender cybercrime, the investigation will study deepfakes using generative artificial intelligence according to wedi (2023). Such an approach demonstrates a fresh thinking on new types of cyber threats and the corresponding necessity to change security strategies. The application and integration of blockchain, and artificial intelligence in the accounting information system as posited in Wanden-Berghe (2023) will also be discussed to underscore the disruption on the conventional triple item.

Also in the scope of this research, Celi (2023) will conduct a systematic review of cybersecurity solutions for IoT network attacks in Latin America. This review will explore approaches from multiple directions and tactics in confronting certain dangers present in that region. We will also take a look at the Alvarado (2022) paper on the survey of machine learning in information security implementation.

Lastly, Lázaro et al will explore the use of the urban security improvement platforms that integrate data science like; artificial intelligence and machine learning (2022). In this more holistic view of security in urban contexts the interconnection between information systems has a major role to play and how these technologies can protect people.

LITERATURE REVIEW

Research of Vidal et al. addresses this in the dynamic intersection between artificial intelligence (AI) and information security. Vidal et al. (2023) organizes the use of AI in organizational settings using UNU University Research as a dissemination platform. This study provides in-depth research on the effectiveness of integrating AI with business security, and reports significant improvements in detecting and responding to threats.

Siñani (2020) on the other hand, describes in detail the use of artificial intelligence, machine learning and deep learning in cybersecurity. Building on a methodological approach grounded in an extensive examination of emerging technologies, which were used to collectively identify the potential capabilities and utilities of these technologies in terms of resilience against cyber threats, we reveal great enhancement in the security architecture when these strategies are employed.

In another dimension, Guerrero & Rodríguez (2023) investigate the impact that technology and artificial intelligence have on the profession of Public Accountant. A methodological approach is used that allows an in-depth study of digital transformation in the accounting industry and to that end understand how artificial intelligence influences traditional functions. The findings point to a new era of disruption in the accounting profession calling for an ongoing re-definition to leverage the benefits of artificial intelligence.

In a related vein, Raraz-Vidal et al. (2023) Investigate the implications of artificial intelligence on health administration with the help of a Peruvian Journal of Health Research© platform. Therefore, the methodological path includes an analysis of examples of cases in health that demonstrates how artificial intelligence modificates the management and administration in this sector, focusing on the huge progress made with respect to increasing efficiency and accuracy of care and healthcare processes.

From another perspective, Iglesias (2023) examines the irruption of artificial intelligence along with information and telecommunications technologies in the security of strategic infrastructures, specifically the electrical system. Through the Scientific Journal of the University Center of the Civil Guard, this study carries out a detailed review of the interaction between artificial intelligence and critical infrastructures, concluding on the need for adaptive security strategies to protect strategic infrastructures.

In another line of research, the Ariza study (2020) on the detection and prevention systems of denial-of-service attacks to the DHCP protocol in a computer network using artificial intelligence techniques, using a doctoral methodology, implies an exhaustive analysis of artificial intelligence techniques applied to network security. The objective is to evaluate the effectiveness of these techniques in the detection and prevention of specific attacks, revealing significant improvements in the response capacity and resistance against denial-of-service attacks.

From another doctoral perspective, Anchundia (2023) contributes to the development of tools based on artificial intelligence for the detection of emails dedicated to phishing. Through a doctoral methodology, the design and

development of a specific tool aim to improve the ability to detect malicious emails, and the results reveal a significant improvement in the accuracy and effectiveness of phishing detection.

Beltrán et al. (2023) provide a safe architecture for training federated and decentralized artificial intelligence models. This paper, published in the Proceedings of the VIII National Cybersecurity Research Conference, focuses on the design and development of a safe framework with the goal of facilitating collaborative training of AI models. The results suggest enhanced security and privacy in the federated and decentralized training method.

In the financial context, Rosero (2023) offers a systematic mapping on the increase in the level of security in the financial information systems of Ecuadorian banking through the use of technologies. Through a systematic analysis of the literature, the objective is to provide an overview of the technologies used to improve banking security, revealing trends and effective approaches to ensure security in financial environments.

In the subject of computer security, Ordoñez (2021) introduces a security system based on STRIDE and AI. The doctorate technique entails designing and implementing a specialized security system based on threat detection using STRIDE. Its aim is to strengthen the ability to detect and mitigate threats in information systems, with results indicating superior performance in detecting and mitigating risks on STRIDE principles.

METHODOLOGY

This research employs a qualitative method of investigation, concentrated on interpretative analysis; meaning that it tries to comprehend how the implementation of AI-based threat detection systems is applied in the security of information systems; trying to provide detailed and deeper understanding. It is a qualitative perspective, which enables the authors to delve into available scientific literature to scrutinize not only on the technical details of AI security but also on perceptions, experiences and evaluations.

RESEARCH DESIGN

The study employs the documentary research, which is a very important tool to thoroughly examine previous literature on AI application in the field of information security. Using this methodology, we hope to acknowledge fresh new methods, trends and strategies that have been applied while designing threat detection systems.

Given this, the study of the documentaries is suitable for a critical evaluation of previous investigations complimenting development of AI based solutions and identifying on chronic loopholes in the domain. This approach provides a systematic picture of the development of technology and its use through time, focusing on how this governs effects on cybersecurity.

DATA SOURCES

The data sources used in the documentary analysis include research articles, dissertations, technical reports and grey literature regarding the application

of AI in cybersecurity. The research papers that selected were those have been published in the last five years, to confirm their relevance and recentness of results focusing on how AI can improve threat detection and maintain data confidentiality and integrity.

We searched for and sourced using familiar scholarly databases such as Scopus, IEEE Explore, Google Scholar and ScienceDirect. We considered research which met the following criteria: (1) research that focused on the application of AI towards information system security, (2) research which evaluated how well methods such as machine learning, deep learning, and neural networks detected threats, and (3) criticism regarding the barriers and opportunities associated with the utilization of AI in cybersecurity which would challenge some dark assumptions.

PROCEDURE

The analysis process evolved over several iterations. The first stage was to conduct a comprehensive literature review using keywords such as artificial intelligence, information systems security, threat detection and machine learning. Next, we selected the larger studies that met our predefined criteria.

All selected references were critically appraised in terms of the methods used, the results obtained and the limitations of every research. The following method of comparison was adopted in order to find the similarities and differences in the use of AI, to highlight the relative advances made in this field at large among all computer security situations.

The critical assessment focused specifically on the performance of AI systems in detecting threats earlier, the flexibility of algorithms to adapt to new trends and on improving information systems resilience. In addition, attention was paid to the ethical issues and problems associated with the use of AI in cybersecurity, that includes matters of data privacy, and algorithmic bias.

ANALYTICAL APPROACH

The interpretative nature of the research allowed, not only for a systematic examination of the documentary data per se, but also to integrate this work into a compelling theoretical proposition for analyzing the data. It gave a deeper, broader understanding of the complexities of the events surrounding cybersecurity and AI.

A thematic analysis was used to identify the emerging and recurring themes in the selected articles, this comprised of subjects such as AI implementation in information security, improvements to threat detection, and AI-painted digital user experiences.

RESULTS

Building threat detection systems with AI proves to be a powerful way of improving the cybersecurity level, particularly in respect of data integrity and confidentiality. In the cybersecurity domain, important aspects supporting AI as an indispensable tool are reinforced by our findings from the extensive

review of scientific literature. The experiment discovered several major details, summarized below.

EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE IN THREAT DETECTION

Perhaps more importantly, the research allows AI-based systems to identify and manage hazards before they occur. They are highly effective systems which are based on machine learning and deep learning algorithms that continue learning to detect more types of cyberattacks, recognize even the smallest anomalies, and do so in real-time. This measure enables the systems to a greater extent to find potential vulnerabilities before someone exploits them.

Most of the courses reviewed within this study reflect that AI is not only faster at detecting threats but also much more efficient than traditional modes. AI-based systems can find intricate threats that be lost in traditional approaches, just by being able to review an enormous amount of data in such short periods of time.

ADAPTABILITY TO EMERGING THREAT PATTERNS

AI can also learn and adjust with the new threat patterns, which is also a significant outcome. The cyber threats mutate rapidly, and our legacy systems which are mainly based on exisiting signatures or rules detection are often easily bypassed by novel types of attacks. Nevertheless, AI based solutions can also alter their operating parameters automatically because they keep learning from data so they can identify brand new threats such as zero day attacks, advanced phishing or spoofing attacks.

The documentary examine suggests that recognize or potential dangers are hundreds of times much more likely to be detected by structures employing adaptive AI than established rule-based technique. It is very important to be flexible in terms of AI behavior in a security context that evolves quickly, ensuring greater information system durability.

IMPROVING THE RESILIENCE OF INFORMATION SYSTEMS

One of the primary advantages of using AI into security systems is that it significantly improves information system resilience. AI algorithms not only detect threats successfully, but they also enable for faster and more accurate incident responses. This equates to a stronger ability to limit and mitigate assaults in real time, decreasing the effect of threats on system operations.

The literature review has also indicated that AI might enhance security incident management by helping to identify the most relevant threats and providing adequate resources to eradicate them. Unlike the prior systems, which are usually inefficient in serves allocation and solving many alarms of security at a real-time.

EFFECTIVENESS OF PERSONALIZING THE USER EXPERIENCE

Naturally, one of the points which figure in the review about AI systems is how it can impact a personalized user experience with applications

and websites to increase both security and usability. Through AI, security measures can automatically adapt based on user behaviors and preferences to change perceived risk levels. It will reduce the friction of going through multiple steps, but not at the cost of loss in data protection.

This result was particularly significant in the context of sensitive applications analogous to financial or government, where not only should security be strong, but it must also remain transparent to the impact on usability user experience.

REDUCTION OF FALSE POSITIVES AND IMPROVEMENT IN OPERATIONAL EFFICIENCY

A significant problem in threat detection systems is the high number of false positives that generates unneeded alerts and can be distracting to operators manning security equipment. An investigation into the matter, however, indicates that AI, in this case particularly deep learning-driven systems can substantially reduce the incidence of false positives. This is owing to its capacity to distinguish between innocuous abnormalities and genuine dangers by assessing many variables and contextual factors.

Decrease of false positives provides a direct impact on operational efficiency, helping security teams to concentrate on the investigation about true threats, fine tuning resource allocation and reducing the response time for highly critical emergencies.

LIMITATIONS IDENTIFIED IN THE IMPLEMENTATION OF AI

Although there were apparent advantages of utilizing AI for information system security, this analysis also highlighted a number of possible limits to its use. These include questions of data privacy, algorithmic bias and the requirement for huge volumes of well-curated data to teach AI models. The fitness of AI algorithms is a considerable problem, as it can lead to both passing under-detection dangers in some situations and event prioritization being incorrect. In the same manner, data privacy is also put at risk when AI systems require access to sensitive information in order to work effectively. These issues need to be addressed by appropriate ethical framework and law to tap into the untapped potential benefits of AI without compromising with privacy and rights.

FUTURE AREAS OF RESEARCH

It also underscored the necessity of addressing glaring gaps through follow up research, most notably in how AI is integrated with other technologies such as blockchain and identifying relevant decision on how to mitigate algorithmic bias and solutions for data privacy issues. It is also encouraged to explore further the prospect of AI improving security in the embedded IoT networks and other emerging technology environments.

Exhibit 1-AI based threat detection system vs Comparison with conventional approaches: The performance score is the benchmark for comparison showing how well a system can detect and neutralize threats

from the cyber world. The data from 2020–2023 will be scored on a scale of 0 to 100, with 100 representing the best possible score.

Over time, we saw AI-powered threat detection systems that achieve performance gain. They got an 85 out of 100 score in 2020 and a higher score of 94 in 2023. It seems the AI systems have learned, over time, to adapt quickly to new threats and changing trends. The continuing expansion of AI systems is due, in part, to the learning capacity and autonomous adaptation seen in such systems.

But the more traditional threat detection systems that often rely on finding known signatures or rules, have shown a much slower evolution compared to AI-powered systems. These systems had a performance score of 70 in 2020 but only reached 75 three years later. This modest increase suggests conventional methods, while helpful, are failing to keep pace with the growing intricacy of cyber threats.

AI-based systems have consistently surpassed traditional systems in terms of performance during the four years analyzed. Whereas in 2020 both scored within 15 points of one another (85 vs. 70), by 2023 this gap had increased to 19 (94 vs. 75). This second metric captures the accuracy and ability of AI solutions to reduce new risks, such as zero-day attacks, advanced phishing attempts and spear phishing.

The chart below clearly depicts how artificial intelligence is transforming the face of cybersecurity environment leading to more powerful, adaptable and efficient systems as compared to tradition means. Like a savior of the day, AI-based Systems to Save Data Integrity and confidentiality in modern digital landscapes, due to the increasing complexity and diversity of cyber threats.

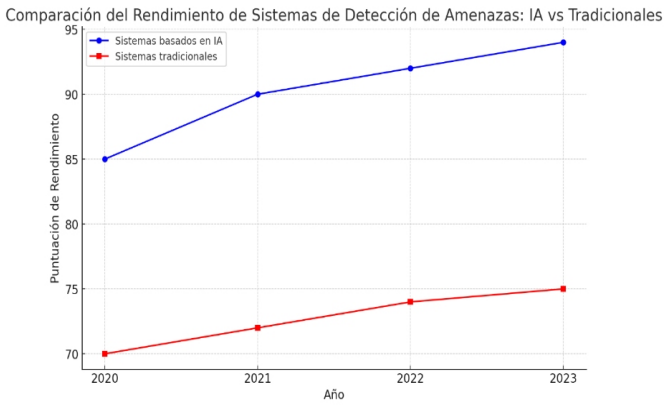

Figure 1: Performance evaluation between AI vs traditional threat detection system.

DISCUSSION

Artificial intelligence (AI) introduction has also brought a great deal of improvement in data security. Vulnerability analysis by Cusme Zambrano and Zambrano Mendoza (2022) using open-source intelligence (OSINT) techniques is an essential component of knowing the threats which may

emerge. In his 2023 paper, Lara looks at the challenges and solutions for securing the network infrastructures and illustrating why companies must execute proactive practices to ensure that data remains unhampered upon in today digital era.

According to Mosquera-Chere (2021), the link between AI and cybersecurity in Ecuador is viewed as an essential connection that must be established simultaneously. This examination highlights the importance of an all-encompassing plan that utilizes the skills of artificial intelligence to protect the confidentiality of data. Cevallos Avilez (2022) contributes to the advancement of detection systems by tackling cyberbullying in digital platforms with an AI-based application.

Pulido (2023) emphasizes the application of generative artificial intelligence in the investigation of gender cybercrime, particularly in light of the rise in deepfakes. This technique displays AI's flexibility to unique challenges, ensuring the integrity of information in the digital world.

Pe Be Iglesias (2023) claims that artificial intelligence has become front and center in setting new standards for securing critical infrastructures, with emphasis centered upon the electric system. The findings, reported in Logos Guardia Civil over the weekend, highlight the need for scalable tools that assure data integrity in critical environments.

These articles provide an exhaustive idea on how artificial intelligence health threat detection systems have grown and evolved. These methods includes the repertoire as vulnerability assessments up to specific cases in cyberbullying and cybercrime situations, demonstrating that AI flexibly implemented as an important resource for ensuring the integrity and confidentiality of information according diverse situations.

CONCLUSION

In the cocktail of studies regarding security of information systems with artificial intelligence, there are key pearls that show why it is essential to analyze in the data from social media also the emotions. Above all, it was decided that threat detection systems driven by artificial intelligence need to be implemented in order to protect information and prevent its release. They are quick at heating to detecting and blocking dangers right away, which makes for an extraordinary venture towards reinforced measures against cyberattacks.

AI can help systems become more resilient, as it can always learn to adapt to new threat patterns. This elastic capability can react to new cybersecurity threats in a digital world that constantly changes. It also illustrates the great potential of generational AI when it comes to uncovering cyber-crimes, and deepfakes in particular. This example highlights the potential of AI, in detecting these sophisticated threats and how crucial it is to preserve data accuracy while doing so using the Internet.

The Connection between AI and Urban Security—Another Key Insight. Data science, AI and machine learning brought safety back to the urban centers. The holistic approach emphasizes the versatility of AI that allows it to transcend across environments and make its presence felt in real life.

Finally, it underscores the need for advanced Latin-American-focused cyber solutions to defend IoT networks and reveals the importance of considering local realities in developing line-of-defense strategies against global threats.

Indeed, the findings made in these studies illustrate how important artificial intelligence is to an information system security. Your ability to learn about it further, and elsewhere, makes its adaptability and the efficacy with which it identifies advanced threats increasingly essential as criminal activities spread across cybercrime to urban security. An important development in computer security trends is the use of sentiment analysis applied to data from social media that stands as a very promising practice contribution other anticipating and counteracting cyber threats. Using Sentiment Analysis, Security professionals can not only just detect threats but they also identify and respond something before it becomes a threat thus making our computer systems more resilient.

ACKNOWLEDGMENT

I would like to express my gratitude to the Pontificia Universidad Católica del Ecuador for their support to carry out the research in the research group Applied Information Systems and Technologies (SITECIA).

REFERENCES

Alvarado, C. (2022). Revisión de la implementación del machine learning en la seguridad de la información.

Anchundia Ronquillo, J. J. (2023). Desarrollo de herramienta basada en inteligencia artificial para la detección de correos electrónicos dedicadas al phishing (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática).

Ariza Palacio, R. D. (2020). Estudio de los sistemas de detección y prevención de ataques de denegación de servicios al protocolo DHCP en una red de computadoras mediante técnicas de inteligencia artificial (Doctoral dissertation, Universidad del Sinú, seccional Cartagena).

Beltrán, E. T. M., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2023). Framework Seguro para Entrenar Modelos de Inteligencia Artificial Federados y Descentralizados. In Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad: Vigo, 21 a 23 de junio de 2023 (pp. 383–390). Universidade de Vigo.

Celi Sandoya, A. M. (2023). Soluciones de ciberseguridad contra los ataques a redes IoT en América Latina, una Revisión Sistemática de la Literatura (Bachelor's thesis).

Cevallos Avilez, I. Z. (2022). Desarrollo de una aplicación basada en inteligencia artificial que detecte el ciberacoso en medios digitales (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática).

Cusme Zambrano, K. D., & Zambrano Mendoza, L. T. (2022). Análisis de vulnerabilidad utilizando herramientas de inteligencia de código abierto (OSINT). Caso de estudio sistemas de información ESPAM MFL (Master's thesis, Calceta: ESPAM MFL).

Guerrero Ruz, O., & Rodríguez Gutiérrez, D. J. (2023). Impacto de la tecnología y la inteligencia artificial en la profesión del Contador Público.

Iglesias, Á. T. L. (2023). Irrupción de la inteligencia artificial junto a las ya no tan nuevas tecnologías de la información y la telecomunicación, en relación a la seguridad de infraestructuras estratégicas-caso particular del sistema eléctrico. Logos Guardia Civil, Revista Científica del Centro Universitario de la Guardia Civil, (1), 103–124.

Lara, G. E. G. (2023). Seguridad en la infraestructura de redes: desafíos y estrategias de protección. Revista Científica y Tecnológica VICTEC, 4(7), 183–192.

Lázaro, G. J. C., Herrera, Q. J. A., Cancho, R. E. D., Roman, C. N. U., Vargas, F. J. I., & Julca, F. J. D. (2022). Implementación De Plataforma De Mejora De La Seguridad Urbana Con Ciencia De Datos, Inteligencia Artificial Y Machine Learning.

Mosquera-Chere, S. O. (2021). La vinculación entre la inteligencia artificial y la seguridad cibernética en el Ecuador. Notas sobre una interconexión necesaria. Polo del Conocimiento, 6(2), 1154–1173.

Ordoñez González, S. A. (2021). Sistema de Seguridad Basado en STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) utilizando inteligencia artificial (Doctoral dissertation, Universidad Autónoma de Nuevo León).

Pulido, I. G. (2023). El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes. IUS ET SCIENTIA, 9(2), 157–180.

Raraz-Vidal, J., Escobedo-Hinostroza, A., & Raraz-Vidal, O. (2023). El impacto de la inteligencia artificial en la administración de la salud. Revista Peruana de Investigación en Salud, 7(4), e2005-e2005.

Rosero Martillo, C. A. (2023). El aumento del nivel de seguridad en los sistemas de información financieros de la banca ecuatoriana mediante el uso de tecnologías: Un mapeo sistemático (Bachelor's thesis).

Sale, J. E., Lohfeld, L. H., & Brazil, K. (2002). Revisiting the quantitative-qualitative debate: Implications for mixed-methods research. Quality and quantity, 36(1), 43–53.

Siñani, C. F. (2020). Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad. INF-FCPN-PGI Revista PGI, 11–13.

Vidal, C. A. V., Centurion, E. S. O., & de los Santos, A. C. M. (2023). Inteligencia artificial en la seguridad de la información en una organización: Artificial intelligence in information security in an organization. Investigación Universitaria UNU, 13(2), 1046–1063.

Wanden-Berghe Fajardo, C. A. (2023). Blockchain e inteligencia artificial en el sistema de información contable: la disrupción de la partida triple.

Yumbo Anís, L. J. (2021). Análisis de técnicas para la detección de amenazas de seguridad utilizando machine learning aplicado a servidores windows server 2016 (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).