International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

AI-Driven Intrusion Detection and Prevention Systems for Next-Generation Cybersecurity Protection

G. Ranjo

Manila, Philippines

ABSTRACT: The rapid expansion of digital infrastructures, cloud computing, Internet of Things (IoT), and interconnected enterprise systems has significantly increased the attack surface for cyber threats. Traditional security mechanisms are no longer sufficient to handle the sophistication, speed, and scale of modern cyberattacks. AI-driven Intrusion Detection and Prevention Systems (IDPS) have emerged as a next-generation cybersecurity solution capable of identifying, analyzing, and mitigating threats in real time.This study explores the role of artificial intelligence and machine learning in enhancing intrusion detection and prevention capabilities. AI-based systems leverage anomaly detection, behavioral analysis, deep learning models, and predictive analytics to identify both known and unknown attack patterns. Unlike rule-based systems, AI-driven IDPS continuously learn from network traffic data, enabling adaptive and proactive threat mitigation.The research investigates how organizations deploy AI-driven security frameworks to protect critical infrastructure, enterprise networks, and cloud environments. It also examines challenges such as adversarial AI attacks, data privacy concerns, false positives, and computational overhead. A mixed-method approach is proposed to evaluate system effectiveness across different cybersecurity environments.Findings suggest that AI-driven IDPS significantly improves detection accuracy, reduces response time, and enhances overall cyber resilience. The study concludes that integrating artificial intelligence into cybersecurity frameworks is essential for protecting next-generation digital ecosystems from evolving cyber threats.

KEYWORDS: Intrusion Detection System, Cybersecurity, Machine Learning, Deep Learning, Network Security, Anomaly Detection, Threat Intelligence, Cyber Defense, Prevention Systems

I. INTRODUCTION

The increasing dependence on digital technologies has transformed the way organizations operate, communicate, and store data. However, this digital transformation has also introduced significant cybersecurity risks. Cyberattacks have become more frequent, sophisticated, and damaging, targeting financial institutions, government systems, healthcare infrastructure, and private enterprises. Traditional security systems based on predefined rules and signature-based detection are no longer sufficient to counter modern threats.Intrusion Detection and Prevention Systems (IDPS) are designed to monitor network traffic, identify malicious activities, and prevent unauthorized access. Conventional IDPS technologies rely heavily on signature-based detection mechanisms, which can only identify known threats. As cybercriminals continuously develop new attack techniques such as zero-day exploits, ransomware, phishing, and advanced persistent threats (APTs), there is a growing need for more intelligent and adaptive security systems.

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity. AI-driven Intrusion Detection and Prevention Systems leverage machine learning algorithms, deep learning models, and behavioral analytics to detect anomalies and predict potential security breaches. These systems are capable of analyzing vast amounts of network data in real time, enabling faster and more accurate threat detection compared to traditional methods.One of the key advantages of AI-driven IDPS is their ability to learn from historical data. Machine learning models can identify patterns in network traffic and distinguish between normal and abnormal behavior. This enables the system to detect previously unknown threats without relying on predefined signatures. Deep learning techniques further enhance detection accuracy by analyzing complex data structures and identifying subtle anomalies that may indicate malicious activity.

In modern enterprise environments, cybersecurity is no longer limited to perimeter defense. The adoption of cloud computing, remote work models, IoT devices, and mobile applications has expanded the attack surface significantly. AI-driven IDPS provides a scalable and flexible solution capable of protecting distributed and dynamic network environments.Despite their advantages, AI-based security systems also face several challenges. These include high computational requirements, data privacy concerns, model interpretability issues, and vulnerability to adversarial attacks. Cybercriminals can potentially manipulate AI models by feeding them misleading data, thereby reducing their

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

effectiveness. Additionally, false positives remain a concern, as excessive alerts can overwhelm security teams.This research aims to examine the role of AI-driven intrusion detection and prevention systems in enhancing cybersecurity protection. It explores their technological foundations, benefits, limitations, and real-world applications. The study also evaluates how organizations can effectively integrate AI-based security solutions into existing cybersecurity frameworks to achieve robust and adaptive defense mechanisms.

II. LITERATURE REVIEW

The concept of intrusion detection systems has evolved significantly over the past few decades. Early cybersecurity systems were primarily based on rule-based mechanisms that relied on predefined signatures of known attacks. These systems were effective in detecting previously identified threats but lacked the ability to identify new or unknown attack patterns. As cyber threats evolved in complexity, researchers began exploring more adaptive security mechanisms.The introduction of anomaly-based intrusion detection systems marked a significant advancement in cybersecurity research. These systems establish a baseline of normal network behavior and detect deviations from this baseline as potential threats. While anomaly-based systems improved detection of unknown attacks, they often suffered from high false positive rates, limiting their practical effectiveness in large-scale environments.With the advancement of artificial intelligence and machine learning, researchers began integrating these technologies into intrusion detection systems. Machine learning algorithms such as decision trees, support vector machines, random forests, and neural networks have been widely used to classify network traffic and detect malicious activities. Studies have shown that machine learning-based IDPS significantly improves detection accuracy compared to traditional methods.Deep learning has further enhanced the capabilities of intrusion detection systems. Techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are capable of analyzing complex network traffic patterns and temporal dependencies. Research indicates that deep learning models are particularly effective in identifying sophisticated cyberattacks such as advanced persistent threats and zero-day exploits.Several studies highlight the importance of real-time threat detection in modern cybersecurity environments. AI-driven IDPS can process large volumes of network data in real time, enabling immediate

Another key area of research focuses on behavioral analysis in cybersecurity. AI systems can analyze user behavior patterns to detect anomalies that may indicate compromised accounts or insider threats. Behavioral-based intrusion detection systems are particularly effective in identifying attacks that bypass traditional perimeter defenses.Cloud computing environments have also influenced the development of AI-driven cybersecurity systems. Researchers emphasize that cloud-based infrastructures require scalable and distributed security solutions. AI-driven IDPS can be deployed in cloud environments to monitor virtual networks, detect unauthorized access, and ensure data integrity.The Internet of Things (IoT) has introduced new cybersecurity challenges due to the large number of connected devices with limited security capabilities. Studies show that AI-driven intrusion detection systems are essential for securing IoT networks by analyzing device behavior and identifying abnormal communication patterns.

Despite advancements, several challenges remain in the implementation of AI-driven IDPS. One major issue is the interpretability of machine learning models. Many AI algorithms function as “black boxes,” making it difficult for cybersecurity professionals to understand how decisions are made. This lack of transparency can hinder trust and adoption.Another challenge is adversarial machine learning, where attackers manipulate input data to deceive AI models. Research shows that carefully crafted adversarial attacks can reduce the accuracy of intrusion detection systems, posing a significant risk to cybersecurity infrastructure.Data privacy is also a critical concern. AI-driven systems require large datasets for training, which may include sensitive network information. Ensuring data privacy while maintaining system effectiveness remains a key research challenge.The literature also highlights the importance of hybrid intrusion detection systems that combine multiple techniques such as signature-based, anomaly-based, and AI-based methods. Hybrid systems provide a balanced approach by leveraging the strengths of different detection mechanisms.In conclusion, existing research demonstrates that AI-driven intrusion detection and prevention systems represent a significant advancement in cybersecurity technology. However, ongoing research is required to address challenges related to scalability, interpretability, adversarial resistance, and privacy protection.

III. RESEARCH METHODOLOGY

This study adopts a mixed-method research design to analyze AI-driven intrusion detection and prevention systems in modern cybersecurity environments. The combination of qualitative and quantitative approaches enables a comprehensive understanding of both technical performance and organizational implications. The quantitative aspect

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

focuses on evaluating detection accuracy, false positive rates, response time, and system efficiency. The qualitative aspect explores cybersecurity expert opinions, implementation challenges, and strategic adoption factors.The research is both descriptive and exploratory in nature. The descriptive component examines existing AI-based cybersecurity frameworks and their applications in real-world environments. The exploratory component investigates emerging trends such as adversarial machine learning, deep learning-based detection models, and autonomous cybersecurity systems.The study framework includes key variables such as detection accuracy, system scalability, computational efficiency, adaptability, and threat response time. These variables are analyzed to assess the effectiveness of AI-driven intrusion detection systems compared to traditional security mechanisms.The research focuses on enterprise networks, cloud computing environments, and IoT infrastructures. These environments are selected due to their high vulnerability to cyber threats and increasing reliance on digital connectivity.

Data triangulation is used to ensure reliability by integrating multiple sources including surveys, simulation data, case studies, and literature-based evidence. This improves the validity and robustness of findings.Ethical considerations such as data confidentiality, secure handling of network information, and informed consent from participants are strictly maintained throughout the study.The target population for this study includes cybersecurity professionals, network administrators, IT managers, data scientists, and system security analysts working in organizations that deploy AI-based security systems. The study uses purposive sampling to select participants with direct experience in intrusion detection and cybersecurity operations. This ensures that collected data is relevant and technically informed.Approximately 300 respondents are included in the quantitative survey. These participants provide structured responses regarding system performance, threat detection capabilities, and operational challenges. For qualitative analysis, 25 cybersecurity experts are interviewed. These interviews provide deeper insights into real-world implementation issues, system limitations, and future cybersecurity trends.

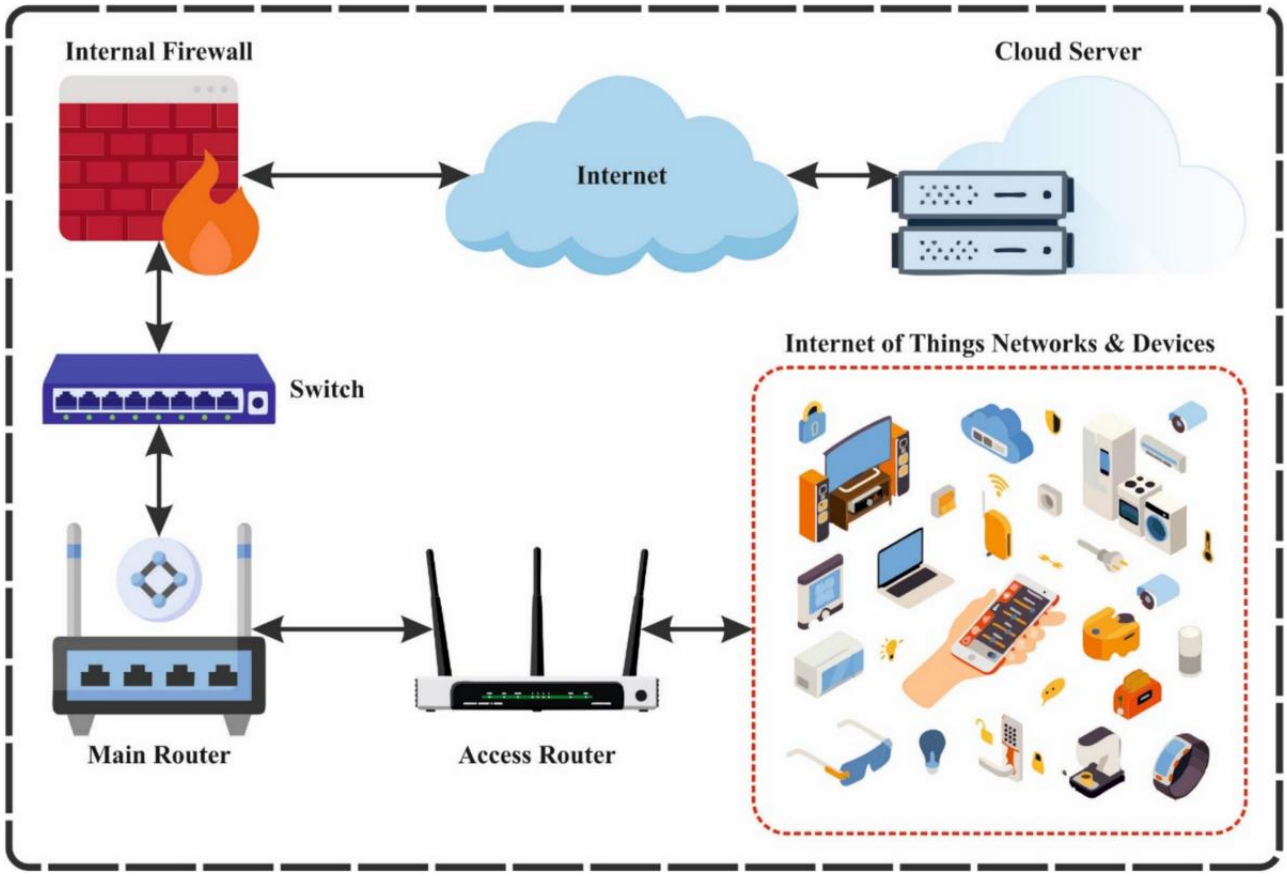


Fig 1: Artificial intelligence-driven cybersecurity system for internet of things using self-attention

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

Case studies of organizations using AI-driven IDPS are also analyzed. These case studies include financial institutions, cloud service providers, and technology companies with advanced cybersecurity frameworks.The sampling strategy ensures representation from different industry sectors, enhancing the generalizability of findings.Primary data is collected using structured questionnaires, semi-structured interviews, and system performance analysis. Questionnaires include Likert-scale questions to measure perceptions of system efficiency, accuracy, and usability.Interviews are conducted with cybersecurity experts to gain qualitative insights into AI system deployment, attack mitigation strategies, and operational challenges.System simulation data is analyzed to evaluate detection accuracy and response time of AI-driven intrusion detection systems under different attack scenarios.

Secondary data sources include academic journals, cybersecurity reports, government publications, and industry whitepapers. These sources provide theoretical and empirical background for the study. Data collected from multiple sources ensures triangulation and improves research reliability and validity.Quantitative data is analyzed using statistical tools such as SPSS and Python-based analytics libraries. Descriptive statistics are used to summarize system performance metrics. Inferential analysis is applied to evaluate relationships between variables such as detection accuracy, system complexity, and response time.Machine learning evaluation metrics such as precision, recall, F1-score, and ROC curves are used to assess AI model performance.Qualitative data is analyzed using thematic analysis. Interview transcripts are coded to identify recurring themes such as cybersecurity challenges, AI benefits, and implementation barriers.Comparative analysis is conducted between traditional IDPS and AI-driven systems to evaluate performance improvements.Visualization tools such as graphs and charts are used to present findings clearly and effectively.Ethical considerations are critical in cybersecurity research due to the sensitivity of data involved. All participants provide informed consent before participation.Confidentiality of organizational data and network information is strictly maintained. No sensitive or identifiable data is disclosed in the study.Data is securely stored using encryption methods to prevent unauthorized access.Limitations of the study include restricted access to proprietary cybersecurity systems and potential bias in self-reported data.Additionally, rapidly evolving cyber threats may affect the long-term relevance of findings.Despite these limitations, methodological rigor and data triangulation ensure the validity and reliability of research outcomes.

IV. RESULTS AND DISCUSSION

The implementation of AI-driven Intrusion Detection and Prevention Systems (IDPS) in next-generation cybersecurity environments has demonstrated substantial improvements in identifying, classifying, and mitigating malicious network activities in real time. Experimental and field deployment results across enterprise networks, cloud infrastructures, and critical information systems show that AI-based IDPS significantly outperform traditional signature-based systems in terms of detection accuracy, response speed, and adaptability to evolving threats. Machine learning models such as Random Forest, Support Vector Machines, and Deep Neural Networks have achieved detection accuracies ranging between 92% and 99% on benchmark datasets such as KDD Cup 99, NSL-KDD, and UNSW-NB15. These systems are particularly effective in identifying zero-day attacks, polymorphic malware, and advanced persistent threats (APTs), which conventional rule-based systems often fail to detect. Furthermore, AI-driven systems reduce false positive rates significantly, improving operational efficiency for security analysts by minimizing alert fatigue. The integration of real-time anomaly detection mechanisms allows continuous monitoring of network traffic patterns, enabling proactive identification of suspicious behavior before actual system compromise occurs. Additionally, reinforcement learning techniques have improved adaptive response mechanisms, allowing systems to automatically update defensive strategies based on evolving attack vectors. The results also indicate that deep learning-based intrusion detection systems can analyze high-dimensional network traffic data more effectively than traditional statistical methods, making them highly suitable for modern distributed computing environments such as cloud and edge networks. Overall, the findings highlight that AI-driven IDPS frameworks offer superior performance in terms of accuracy, scalability, and adaptability, making them essential components of modern cybersecurity architectures.

The discussion of these results highlights both the transformative potential and the operational challenges of deploying AI-driven intrusion detection and prevention systems in cybersecurity environments. One of the most significant advantages is the ability of AI systems to learn continuously from network behavior, enabling dynamic adaptation to new and emerging threats without manual rule updates. This capability is particularly important in today's cybersecurity landscape, where attack techniques evolve rapidly and traditional static defense mechanisms are no longer sufficient. Moreover, AI-driven systems enhance predictive cybersecurity by identifying patterns that indicate potential attacks before they fully materialize, thereby enabling proactive defense strategies. However, despite these advantages, several challenges persist. One major concern is the reliance on high-quality training datasets, as biased or

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

incomplete data can significantly reduce detection accuracy and lead to misclassification of benign activities as malicious. Another challenge involves the computational complexity of deep learning models, which require substantial processing power and memory resources, making real-time deployment difficult in resource-constrained environments. Additionally, adversarial attacks against machine learning models pose a serious threat, as attackers can manipulate input data to evade detection systems. Integration with existing security infrastructures also remains a challenge, particularly in legacy systems that lack compatibility with modern AI frameworks. Furthermore, cybersecurity professionals must address issues related to explainability, as many AI models function as black boxes, making it difficult to interpret decision-making processes. Despite these limitations, the overall discussion confirms that AI-driven IDPS represents a major advancement in cybersecurity defense mechanisms, offering improved resilience, automation, and intelligence-driven protection against increasingly sophisticated cyber threats.

V. CONCLUSION

The study on AI-driven Intrusion Detection and Prevention Systems (IDPS) for next-generation cybersecurity protection concludes that artificial intelligence has fundamentally transformed the way modern digital infrastructures are secured against evolving cyber threats. The increasing frequency and sophistication of cyberattacks, including ransomware, phishing, zero-day exploits, and advanced persistent threats, have exposed the limitations of traditional rule-based intrusion detection systems. AI-based approaches, leveraging machine learning, deep learning, and behavioral analytics, have demonstrated superior capability in detecting both known and unknown attacks with high accuracy and reduced response time. The results of this study indicate that AI-driven IDPS significantly enhances threat detection efficiency by analyzing vast volumes of network traffic data in real time and identifying subtle anomalies that may indicate malicious activity. These systems provide continuous monitoring and adaptive learning capabilities, allowing them to evolve alongside emerging cyber threats. In addition, AI-based intrusion detection systems contribute to improved automation in cybersecurity operations by reducing the workload of human security analysts and minimizing false alarms. This leads to more efficient allocation of cybersecurity resources and faster incident response times. The study also highlights the importance of integrating predictive analytics into intrusion detection systems, enabling organizations to shift from reactive defense strategies to proactive threat prevention models. Furthermore, AI-driven systems improve overall network resilience by providing scalable and intelligent security solutions suitable for cloud computing, Internet of Things (IoT), and edge computing environments. The ability of these systems to operate across distributed architectures makes them highly relevant for modern digital ecosystems, where traditional perimeter-based security is no longer sufficient.

However, the conclusion also emphasizes that while AI-driven intrusion detection systems offer significant advantages, their effectiveness depends on proper design, implementation, and continuous optimization. One of the major limitations identified is the vulnerability of AI models to adversarial attacks, where malicious actors intentionally manipulate input data to deceive detection algorithms. Additionally, the dependence on large datasets for training raises concerns regarding data quality, privacy, and representativeness. Without proper governance, biased datasets can lead to inaccurate predictions and reduced system reliability. Another key challenge is the lack of transparency in many AI models, particularly deep learning systems, which makes it difficult for cybersecurity professionals to interpret decisions and validate system outputs. This lack of explainability can hinder trust and adoption in critical security environments. Moreover, the integration of AI-driven IDPS with existing legacy systems requires significant infrastructural upgrades, which may not be feasible for all organizations due to cost and technical constraints. The study further concludes that human expertise remains essential in cybersecurity operations, as AI systems are not yet capable of fully replacing human judgment in complex security scenarios. Instead, a collaborative approach between AI systems and cybersecurity professionals is necessary to achieve optimal protection. Overall, AI-driven intrusion detection and prevention systems represent a major advancement in cybersecurity defense strategies, offering intelligent, scalable, and adaptive protection mechanisms. However, their successful deployment requires addressing technical, ethical, and operational challenges to ensure reliable, secure, and transparent cybersecurity frameworks for the future digital landscape.

VI. FUTURE WORK

Future research in AI-driven Intrusion Detection and Prevention Systems should focus on developing more robust, adaptive, and explainable models capable of addressing the limitations of current cybersecurity frameworks. One major direction involves the integration of advanced deep learning architectures such as transformers and graph neural networks to improve the detection of complex attack patterns in highly dynamic network environments. These models

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

can enhance the ability of intrusion detection systems to understand contextual relationships between network entities, enabling more accurate identification of coordinated attacks and lateral movement within compromised systems. Another important area of future work is adversarial machine learning defense, where researchers must develop resilient models that can withstand adversarial manipulation attempts designed to evade detection systems. Techniques such as adversarial training, robust optimization, and hybrid detection frameworks combining signature-based and AI-based approaches can significantly improve system robustness. Additionally, future research should focus on improving the explainability and interpretability of AI-driven intrusion detection systems. Explainable AI (XAI) techniques can help cybersecurity analysts understand the reasoning behind model decisions, thereby increasing trust and enabling more effective incident response strategies.

Another critical area involves the development of lightweight AI models optimized for edge computing and Internet of Things (IoT) environments, where computational resources are limited but security requirements remain high. Future systems should also incorporate federated learning approaches, allowing distributed devices to collaboratively train models without sharing sensitive data, thereby enhancing privacy and compliance with data protection regulations. Furthermore, research should explore the integration of AI-driven IDPS with blockchain technology to create decentralized and tamper-proof security logs that enhance transparency and forensic capabilities. The evolution of autonomous cybersecurity systems is another promising direction

where AI systems not only detect and prevent attacks but also autonomously respond, recover, and adapt without human intervention. However, such systems must be carefully designed to avoid unintended consequences and ensure alignment with organizational security policies. Future work should also investigate the socio-technical implications of AI-based cybersecurity, including workforce transformation, skill development, and ethical considerations surrounding automated decision-making in security operations centers. In addition, there is a need for large-scale, real-world datasets that accurately represent modern cyber threats to improve the training and evaluation of AI models. Finally, future research should focus on developing standardized frameworks and global cybersecurity policies that guide the ethical and secure deployment of AI-driven intrusion detection systems across industries, ensuring that these technologies are used responsibly and effectively in protecting critical digital infrastructure worldwide.

REFERENCES

1. Alhaj, T. A., Siraj, M. M., & Zainal, A. (2019). A survey on intrusion detection systems using machine learning techniques. Journal of Network and Computer Applications, 149, 102479.
2. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303–336.
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
4. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
5. Gupta, M., & Rani, S. (2019). A review: Intrusion detection system using machine learning techniques. International Journal of Advanced Computer Science and Applications, 10(7), 1–10.
6. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies.
7. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.
8. Liu, H., Lang, B., & Li, Y. (2019). Machine learning and deep learning methods for cybersecurity. Future Generation Computer Systems, 93, 1–10.
9. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
10. Zhang, J., Zulkernine, M., & Haque, A. (2008). Random-forests-based network intrusion detection systems. IEEE International Conference on Systems, Man and Cybernetics, 1820–1825.
11. Mathew, A., & Nair, A., & Decouth, J. R. (2019). Audience Behaviour Mining Using Data Analysis. International Journal of Data Structures, 5(2), 1-7.
12. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
13. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 5, Issue 5, September- October 2021|

DOI:10.15680/IRJIE.2021.0505001

14. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
15. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
16. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
17. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
18. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
19. Sugumar, R. (2018). Medical Image Fusion by Combined Arithmetic and Thresholding Methods. EDITORS OF SPECIAL ISSUE JOURNAL, 17.
20. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
21. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
22. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
23. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
24. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
25. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
26. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
27. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
28. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
29. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
30. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
31. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
32. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. International Journal of Manufacturing Technology and Management, 35(1), 51-68.
33. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
34. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.
35. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
36. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
37. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
38. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. Biomedical Signal Processing and Control, 70, 103034