International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
***Article Received:** 25 December 2023 **Revised:** 12 January 2024 **Accepted:** 20 February 2024*

Intrusion Detection and Prevention for Cloud Security

Amit Goswami[1], Ripalkumar Patel[2], Chirag Mavani[3], Hirenkumar Kamleshbhai Mistry[4]
[1]Software developer, Source Infotech
[2]Software developer, Emonics
[3]Devops engineer, Dxc Technology
[4]Sr. System Administrator, Zenosys LLC
amitbspp123@gmail.com[1], Ripalpatel1451@gmail.com[2], chiragmavanii@gmail.com[3], hiren_mistry1978@yahoo.com[4]

***Abstract**:* This paper consultation presents a technique for creating a layered taxonomy of Intrusion Location and Prevention Frameworks (IDPS). The strategy methodically classifies IDPSs based on their utility components, research strategies, layout plans, and mechanical systems. Through the introduction of a comprehensive written study, keynote and real cases, the scientific classification presents an organized system that improves the understanding and application of IDPS in various security situations, and especially emphasizes their contribution to cloud security. This study contributes to the advancement of IDPS classification, advertising experiences in and education research, and the thought of implementing cyber security methods.

***Keywords:** IDPS, intrusion detection, intrusion prevention, layered taxonomy, cybersecurity.*

1. INTRODUCTION

The cloud benefit has totally molded the data innovation scene, advertising phenomenal versatility, adaptability and effectiveness in overseeing and preparing information. In any case, as organizations move increasingly of their operations and information to the cloud, the scene of cybersecurity challenges is advancing in parallel. Interruption discovery and anticipation frameworks (IDPS) have developed as basic components in securing cloud situations from a assortment of dangers, from conventional cyber assaults to modern, focused on interruptions. This introduction investigates the significance of IDPS to cloud security and gives an outline of their parts, challenges and advancing elements within the cloud biological system.

Cloud environments, characterized by their dynamic and distributed nature, present unique security challenges compared to traditional on-premise infrastructures. The flexibility and multi-tenant architecture of the cloud is useful for resource management, but also creates vulnerabilities that can be exploited by malicious actors. Unlike static networks, cloud infrastructures can scale up or down quickly, allocate resources dynamically and support many interconnected services. This fluidity, while essential for cloud operations, makes traditional security measures difficult and ineffective.

IDS and IPS are an in a general sense part of any strong security framework. An IDS is arranged to screen and analyze organize movement for signs of harmful activity, creating cautions when suspicious plans are recognized. (IPS) do more than fair recognize dangers; they moreover take robotized activities to avoid or decrease them. In cloud security, Intrusion Detection and Prevention Systems (IDPS) must adjust to the cloud's tremendous and computerized nature. This implies moving from ancient strategies of finding dangers to modern ones that can spot abnormal designs.

IDPS plays a key part in cloud security by acting as the primary line of defense against different cyber dangers like information breaches, unauthorized get to, malware, and DDoS assaults. They screen activity between cloud administrations, virtual machines, and client gadgets to spot unordinary action that might demonstrate an assault. When coordinates with cloud administration devices, they can identify and react to dangers in real-time, indeed in complex cloud frameworks.

However, utilizing IDPS within the cloud is challenging. Cloud setups can be complicated, counting open, private, and crossover models, each requiring diverse IDPS solutions. The tall information and organize activity within the cloud can overpower conventional IDPS, driving to slowdowns and wrong cautions. This requires IDPS to be adaptable and able to handle expansive information volumes proficiently.

Another challenge is joining IDPS with existing security frameworks and assembly compliance necessities. Organizations regularly have strict rules requiring particular security measures. IDPS must give clear perceivability into cloud operations and screen scrambled activity, utilizing procedures like profound parcel review (DPI) and machine learning, without breaking encryption rules to preserve compliance and security.

As cloud innovation and cyber dangers advance, IDPS strategies must persistently progress. Conventional signature-based discovery strategies based on known designs of noxious behavior are progressively lacking against modern dangers that utilize advanced avoidance methods. Since of this, present day IDPS frameworks incorporate behavioral investigation and inconsistency location to identify deviations from typical operation which will show an assault.

Machine learning calculations play a basic part in this approach, permitting IDPS to memorize from chronicled information and adjust to modern dangers in genuine time. This energetic and proactive approach moves forward IDPS' capacity to distinguish and relieve dangers some time recently they can cause noteworthy harm. In expansion, the development of cloud-based security arrangements has changed the scene of interruption location and avoidance. Cloud-based IDPSs are outlined to work consistently in cloud situations, leveraging cloud platform-specific highlights such as auto-scaling, micro-segmentation and holders. These arrangements are profoundly customizable and can be coordinates with cloud administrations and applications to supply relevant security. For case, in a holder environment, a cloud-based IDPS can screen intelligent between holders and identify peculiarities characteristic of holder workloads. This near observing makes strides the generally security of cloud applications by making it more troublesome to misuse vulnerabilities. Joining IDPS with cloud security data and occasion administration (SIEM) assist increments their viability. SIEM frameworks collect and analyze security data from different sources and give a bound together diagram of the data security environment. Combined with IDPS, SIEM frameworks can connect interruption alarms with other security occasions, empowering more comprehensive risk investigation and response. This integration encourages quicker occurrence location and reaction, diminishing the potential affect of security breaches on cloud operations. In expansion, it bolsters the mechanization of data security workflows, permitting organizations to reply to dangers with negligible human mediation.

Intrusion area and expectation systems are invaluable gadgets inside the cloud security weapons store. As organizations continue to get a handle on cloud computing, the require for an effective IDPS gets to be dynamically basic to guarantee against progressing cyber perils. The curiously characteristics of cloud circumstances require inventive IDPS courses of action that can be reliably scaled, balanced and coordinates with cloud systems. Cutting edge IDPS offers advanced advancements such as machine learning, behavioral analytics and cloud-based capabilities to supply overwhelming affirmation against a wide amplify of security challenges. As the cloud continues to development, the strategies and developments utilized to secure it must besides ensure that organizations can take full advantage of the cloud's potential though keeping up incredible security.

2. REVIEW OF WORKS

Intrusion detection and prevention systems (IDPS) are critical to securing inherently complex and dynamic cloud environments. The literature offers a variety of perspectives and methods that reflect the evolving nature of cloud cybersecurity. This review examines the most important works and state-of-the-art approaches in this field, highlighting the contributions of various authors to the understanding and development of IDPS for cloud security.

2.1 Early Foundations of Intrusion Detection

A seminal article by the SANS Institute (2001) defines the basic principles and operating mechanisms of intrusion detection systems (IDS). This early mapping highlights the need for IDS to detect unauthorized access and other security breaches, laying the foundation for IDS operation in broader security architectures. Although the context was not specifically adapted to cloud environments, the principles presented are still relevant and will inform the future development of IDPS technology. C. Lawrence (2004) expands the discussion predicting the development of IPS (Intrusion Prevention Systems) as a natural successor of IDS. Lawrence emphasizes the proactive ability of IPS to not only detect but also prevent intrusions, marking a significant shift in intrusion management strategies. This work requires the integration of detection and prevention capabilities that have become increasingly prominent in cloud security solutions.

2.2 Cloud-Specific Intrusion Detection and Prevention

A. Zarrabi and A. Zarrabi (2012) make an important contribution to the understanding of IDPS in cloud environments. Their research examines the deployment of Internet Intrusion Detection System (IIDS) services in cloud infrastructures, focusing on the unique challenges presented by the distributed nature of the cloud. They stretch the ought to alter conventional Interruption Discovery Framework (IDS) strategies for cloud situations since of the adaptable and changing nature of cloud administrations. The National

Institute of Standards and Technology (NIST) gives nitty gritty direction on IDPS in a paper by K. Scarfone and P. Mell (2007). Their paper investigates different IDPS models and their utilize in cloud situations. Typically a key reference for understanding how IDPS works and is actualized within the cloud. M. Boniface and colleagues (2010) talk about the challenges of coordination IDPS into Platform-as-a-Service (PaaS) frameworks. They propose a unused PaaS plan that permits for real-time quality benefit administration, counting security observing. Their work outlines the interaction between benefit conveyance and security in cloud stages and gives understanding into how IDPS can be consistently coordinates into cloud benefit structures.

2.3 Advanced Detection Techniques and Challenges

Advancing danger pictures require progressed location methods, such as G. Carl et al. (2006). They investigate distinctive strategies to distinguish Dissent of Benefit (DoS) assaults, which are especially vital in cloud situations where benefit accessibility is basic. Their work emphasizes the significance of strong irregularity location instruments to decrease the affect of DoS assaults on cloud administrations. X.D. Hoang et al. (2009) show a software-based irregularity location framework that employments numerous location motors and fluffy thinking. This approach employments a assortment of location strategies to make strides the precision and unwavering quality of interruption discovery, tending to untrue positives and the ought to identify an exact irregularity in cloud systems. G.Thatte et al. (2011) center on parametric strategies for total street client dedetection, giving a quantitative system for identifying deviations from ordinary activity designs. Their work emphasizes the application of factual models to cloud arrange activity observing, which contributes to the advancement of versatile and proficient irregularity discovery frameworks. H. T. Elshoush and I. M. Osman (2011) examine impedances relationship methods in agreeable shrewdly interruption discovery frameworks. They emphasize the significance of coordination impedances relationship components to make strides the productivity of IDPS, particularly in cloud situations where different location frameworks work at the same time. Their work gives a guide for creating cleverly and collaborative IDPS arrangements that can adjust to the complex risk scene of cloud computing.

2.4 Integration of Machine Learning and Artificial Intelligence

The integration of machine learning and fake experiences in IDPS is a crucial step in cloud security. T. Pietraszek look at the application of data mining and machine learning methods to diminish unfaithful positives in intrusion area. Their work lays the premise for counting flexible learning calculations to IDPS, allowing these systems to progress and move forward their affirmation over time. A. Patcha and J.-M. Halt (2007) gives a graph of irregularity area strategies, highlighting the foremost later mechanical designs and existing courses of action. Their comprehensive audit incorporates talks of machine learning calculations and their pertinence to interruption discovery, and gives understanding into how these methods can be adjusted to address the special challenges of cloud security. R. Perdisci et al. (2006) examined caution clustering methods for interruption discovery frameworks, centering on lessening the cognitive stack of security examiners by gathering related cautions. This approach employments machine learning to recognize designs and relationships between interruption cautions, encouraging more successful and productive danger reaction instruments in cloud situations. Ayyalasomayajula et al., in their research work published in 2019, provided key insights into the cost-effectiveness of deploying machine learning workloads in public clouds and the value of using AutoML technologies. Ayyalasomayajula et al., 2021, provided an in-depth review of proactive scaling strategies to optimize costs in cloud-based hyperparameter optimization for machine learning models. Authors Boozary, Payam et. al. discussed the impact of marketing automation on consumer buying behavior in the digital space via artificial intelligence.

2.5 Collaborative and Distributed Detection Systems

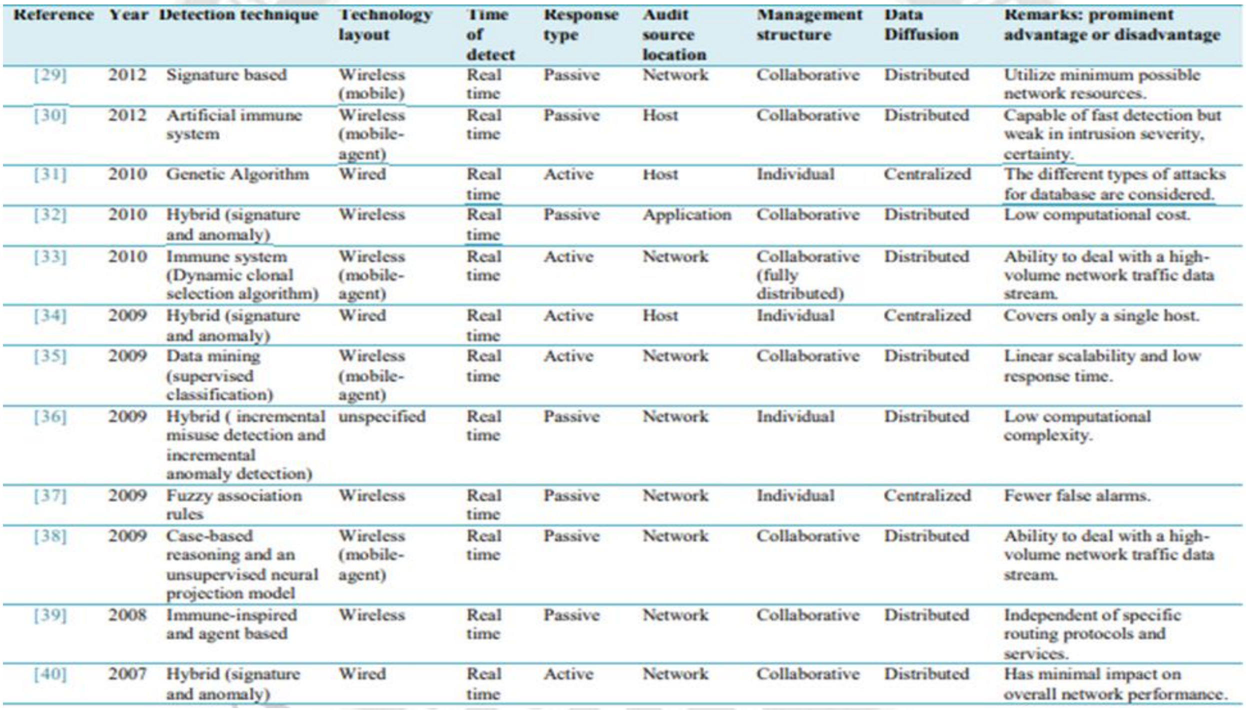
The move towards collaborative and dispersed discovery frameworks is another basic zone of improvement in IDPS. C. V. Zhou et al. (2010) overview facilitated assaults and collaborative interruption discovery techniques, emphasizing the require for coordinates approaches to distinguish and relieve complex, multi-faceted dangers. Their work highlights the significance of collaboration among diverse location frameworks and partners in keeping up strong cloud security. Y. Li et al. (2010) propose a conveyed interruption location strategy based on safe portable specialist frameworks. Their approach utilizes independent operators to screen and analyze arrange activity over disseminated cloud situations, giving a adaptable arrangement for real-time interruption location. This work outlines the potential of disseminated and independent frameworks in improving the nimbleness and responsiveness of IDPS within the cloud. O. Awodele et al. (2009) appear a multi-layered approach to arranging brilliantly intrusion area and shirking systems. They advocate for a layered security appear that planning distinctive location methods and propels to supply comprehensive security against a wide run of threats. Their work underscores the require of grasping a all enveloping approach to IDPS arrange, particularly in complex cloud circumstances where diverse layers of defense are required.

2.6 Practical Applications and Case Studies

Directly to on-the-ground applications and case scenarios, it donates useful encounters to the actual operation and practicality of IDPS. M. Leitner et al. (2007) study disordering based on peer-to-peer perfect models based on a quasi-Celtic migration from Madeira. Their work describes the application of peer-to-peer propellers to control and mitigate security situations, contributing to a reasonable perspective for IDPS delivery in cloud devices.

J. E. Gaffney Jr. and J. W. Ulvila (2001) review the valuation of disturbance locators using option speculation. Their case consider highlights the challenges and contemplations included in inquiring about how IDPS works and how valuable it is, giving a system for assessing the run of these frameworks in real-world circumstances.

A. Patel and colleagues (2010) provide a nitty gritty outline of frameworks that distinguish and avoid interruptions. They give data on how well these frameworks work and offer thoughts on their execution. Their work offers a wide see of distinctive IDPS models and strategies, serving as a pivotal asset for understanding how these frameworks work in cloud situations.



Reference	Year	Detection technique	Technology layout	Time of detect	Response type	Audit source location	Management structure	Data Diffusion	Remarks: prominent advantage or disadvantage
[29]	2012	Signature based	Wireless (mobile)	Real time	Passive	Network	Collaborative	Distributed	Utilize minimum possible network resources.
[30]	2012	Artificial immune system	Wireless (mobile-agent)	Real time	Passive	Host	Collaborative	Distributed	Capable of fast detection but weak in intrusion severity, certainty.
[31]	2010	Genetic Algorithm	Wired	Real time	Active	Host	Individual	Centralized	The different types of attacks for database are considered.
[32]	2010	Hybrid (signature and anomaly)	Wireless	Real time	Passive	Application	Collaborative	Distributed	Low computational cost.
[33]	2010	Immune system (Dynamic clonal selection algorithm)	Wireless (mobile-agent)	Real time	Active	Network	Collaborative (fully distributed)	Distributed	Ability to deal with a high-volume network traffic data stream.
[34]	2009	Hybrid (signature and anomaly)	Wired	Real time	Active	Host	Individual	Centralized	Covers only a single host.
[35]	2009	Data mining (supervised classification)	Wireless (mobile-agent)	Real time	Active	Network	Collaborative	Distributed	Linear scalability and low response time.
[36]	2009	Hybrid (incremental misuse detection and incremental anomaly detection)	unspecified	Real time	Passive	Network	Individual	Distributed	Low computational complexity.
[37]	2009	Fuzzy association rules	Wireless	Real time	Passive	Network	Individual	Centralized	Fewer false alarms.
[38]	2009	Case-based reasoning and an unsupervised neural projection model	Wireless (mobile-agent)	Real time	Passive	Network	Collaborative	Distributed	Ability to deal with a high-volume network traffic data stream.
[39]	2008	Immune-inspired and agent based	Wireless	Real time	Passive	Network	Collaborative	Distributed	Independent of specific routing protocols and services.
[40]	2007	Hybrid (signature and anomaly)	Wired	Real time	Active	Network	Collaborative	Distributed	Has minimal impact on overall network performance.

Table 1. Classification of existing IDPSs based on a layered-taxonomy

3. METHODOLOGY FOR DEVELOPING A LAYERED-TAXONOMY OF INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

A precise approach was attempted to create a layered taxonomy of Disruption Location and Avoidance Frameworks (IDPS). Initially, clear objectives and scope were established, with a focus on creating an organized classification that encompasses the various IDPSs based on their components, search strategies, organizational patterns, and innovative systems. At that time, a comprehensive literature review was conducted, including scientific articles, industry reports and definitive benchmarks. This review distinguished key highlights such as positioning instruments (eg, signature-based, anomaly-based), delivery procedures (eg, web-based, hosted), and innovation integration (eg, machine learning, collaborative positioning).

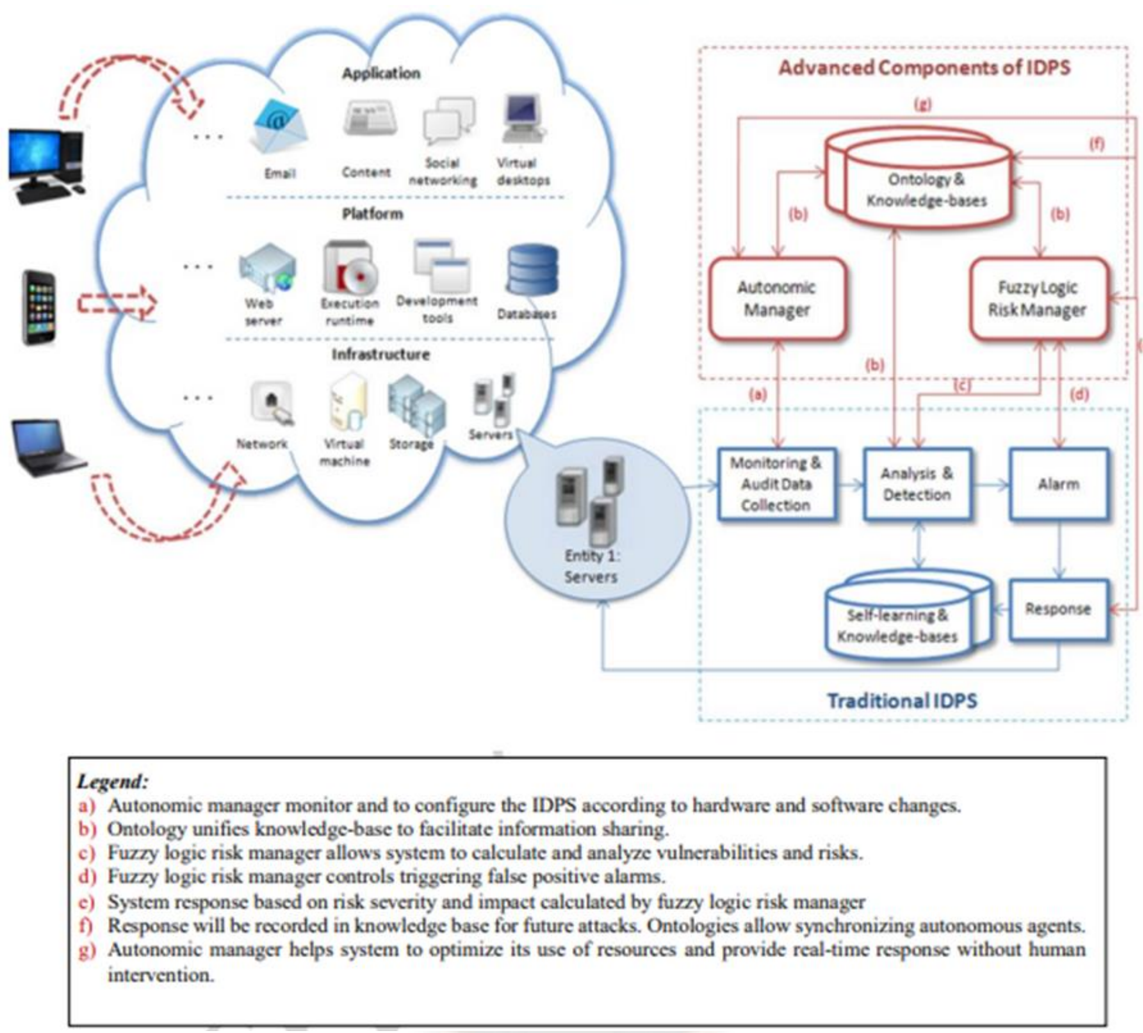
Utilizing the information from the investigate, a draft logical classification was made, gathering IDPS into layers based

Article Received: *25 December 2023* ***Revised:*** *12 January 2024* ***Accepted:*** *20 February 2024*

on their utility and capacities. This draft was refined with master input and real-world illustrations to guarantee its viable pertinence and precision. At last, a formal classification was created, giving a clear, layered framework for understanding and applying IDPS in different scenarios, particularly in cloud security. This organized approach guarantees the taxonomy's strength and pertinence in both the scholarly community and industry.

4. RESULTS

The development of a layered taxonomy of Intrusion Detection and Prevention Systems (IDPS) results in a robust classification system that organizes different IDPS into layers based on their functional roles, detection methods, application architectures, and technical frameworks. This structured system includes several layers, each focusing on specific aspects of IDPS.



Legend:
a) Autonomic manager monitor and to configure the IDPS according to hardware and software changes.
b) Ontology unifies knowledge-base to facilitate information sharing.
c) Fuzzy logic risk manager allows system to calculate and analyze vulnerabilities and risks.
d) Fuzzy logic risk manager controls triggering false positive alarms.
e) System response based on risk severity and impact calculated by fuzzy logic risk manager
f) Response will be recorded in knowledge base for future attacks. Ontologies allow synchronizing autonomous agents.
g) Autonomic manager helps system to optimize its use of resources and provide real-time response without human intervention.

Fig.1: A typical IDPS for one of the entities within cloud computing

These incorporate fundamental discovery instruments like signature- and anomaly-based frameworks, progressed procedures coordination machine learning and collaborative location, and sending methodologies covering web-based, host-based, and cloud-based applications. This layered approach gives an all-encompassing see of the IDPS environment, reflecting the differing qualities and complexity of these frameworks. Figure 1 outlines a commonplace IDPS setup for a single cloud benefit unit.

The scientific categorization effectively covers a wide extend of IDPS strategies, including both conventional frameworks and present day propels. Joining diverse operational settings and mechanical advancements, especially within the field of cloud security, the scientific classification addresses the advancing nature of IDPS. This comprehensive system guarantees that the scientific categorization remains pertinent to unused dangers and innovations and gives understanding into both built up and

***Article Received:** 25 December 2023 **Revised:** 12 January 2024 **Accepted:** 20 February 2024*

state-of-the-art IDPS hones. In Figure 2 A layered scientific categorization of IDPS is delineated.

Approval of the scientific categorization utilizing genuine case considers and master input affirmed its down to earth pertinence and precision. By mapping existing IDPS arrangements to the proposed levels, the scientific categorization illustrated its convenience in classifying and understanding current IDPS advances. Master interviews advance refined the classification criteria, expanding the pertinence of the scientific categorization and guaranteeing that it viably captures the subtleties of the different applications of the IDPS. This approval prepare made the scientific categorization a solid instrument for analyzing and creating IDPS arrangements.

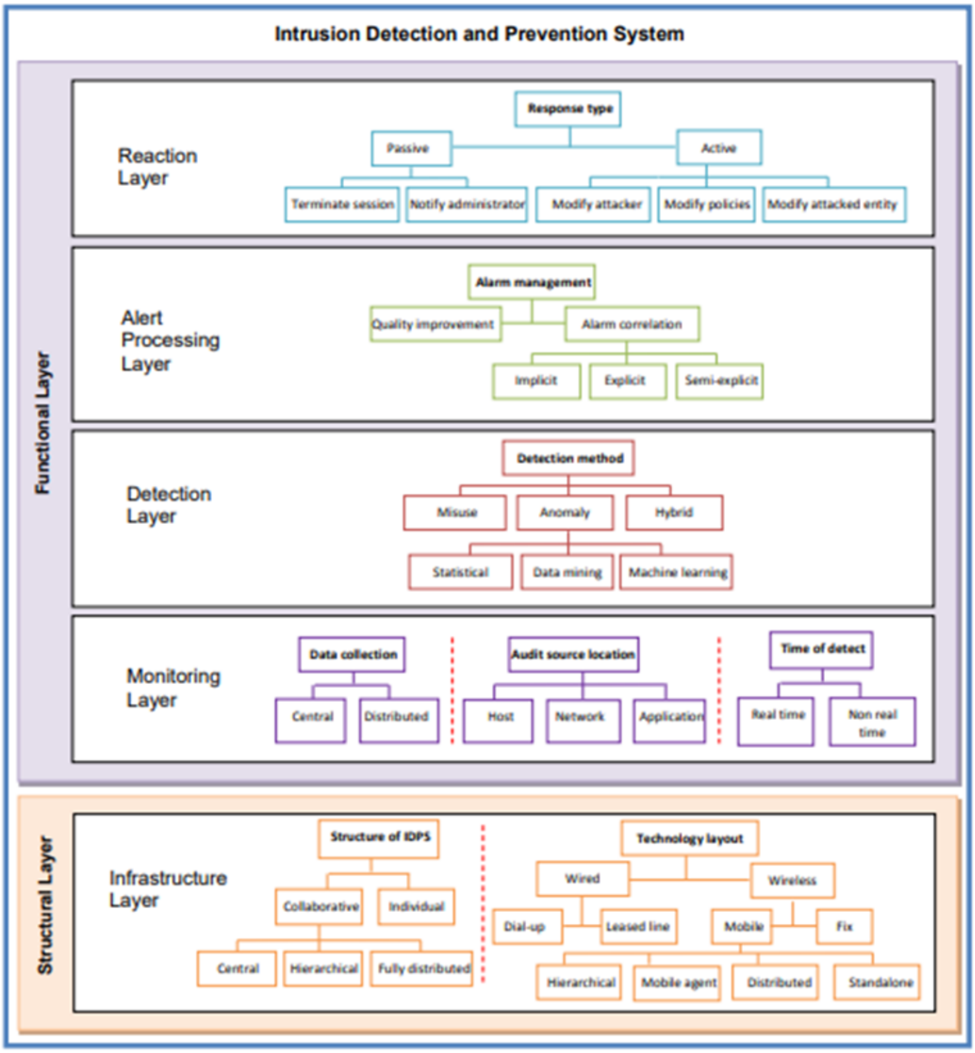


Fig.2: A layered-taxonomy of IDPS

The extreme documentation of the logical categorization gives point by point delineations of each layer and the criteria utilized for classification. This documentation not because it were clarifies the structure and reason of the logical categorization but as well offers practical direction for its application in numerous circumstances. By clarifying the qualifications between diverse sorts of IDPS and their individual layers, the scientific categorization helps analysts and specialists in selecting and executing suitable IDPS methodologies. This organized approach improves the capacity to address security challenges in diverse settings, especially within the setting of cloud security, where the integration of different IDPS innovations is pivotal for compelling danger discovery and avoidance.

In general, the layered-taxonomy gives a comprehensive and down to earth system for understanding and applying IDPS. It serves as a important asset for both scholastic investigate and industry hone, supporting the development of more viable and versatile IDPS arrangements within the confront of advancing security dangers.

6. CONCLUSION

The advancement of a layered-taxonomy for Interruption Location and Anticipation Frameworks (IDPS) has yielded a comprehensive classification system that successfully categorizes different IDPS based on their useful parts, location strategies, arrangement designs, and mechanical systems. This scientific categorization obliges both conventional and present day IDPS, tending to their application in differing situations, especially in cloud security. Through precise writing audit, master criticism, and approval against real-world cases, the scientific classification has demonstrated to be a vigorous instrument for understanding, analyzing, and actualizing IDPS. It gives profitable bits of knowledge for analysts and professionals, upgrading the capability to create and apply successful IDPS methodologies within the quickly advancing scene of cybersecurity.

REFERENCES

[1]. Premkumar Reddy, Yemi Adetuwo and Anil Kumar Jakkani, Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks, International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp.25-34. doi: https://doi.org/10.17605/OSF.IO/52RHK

[2]. A. Zarrabi and A. Zarrabi, "Internet Intrusion Detection System Service in a Cloud," IJCSI International Journal of Computer Science, vol. 9, no. 5, 2012.

[3]. C. Lawrence, "Intrusion Prevention Systems: The Future of Intrusion Detection," in Intrusion Prevention Systems: The Future of Intrusion Detection, Auckland, 2004.

[4]. Adeola Agbonyin, Premkumar Reddy, Anil Kumar Jakkani, Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES), International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp. 182-191. doi: https://doi.org/10.17605/OSF.IO/QX3DP

[5]. M. Boniface, B. Nasser, J. Papay and S. C. Phillips, "Platform-as-aService Architecture for Real-Time Quality of Service Management in Clouds," in Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on, Barcelona, 2010.

[6]. A. Ziarati, ""A multilevel evolutionary algorithm for optimizing numerical functions"," IJIEC, vol. 2, 2011.

[7]. G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10, pp. 82-89, 2006.

[8]. A. Sixsmith and N. Johnson, "A smart sensor to detect the falls of the elderly," Pervasive Computing, IEEE, vol. 3, pp. 42-47, 2004.

[9]. M. E. Whitman and H. J. Mattord, "Principles of information security," ed: Course Technology Ptr, 2011, p. 315.

[10]. K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," NIST Special Publication, vol. 800, p. 94, 2007.

[11]. A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," Information Management & Computer Security, vol. 18, pp. 277-290, 2010.

[12]. G. Thatte, U. Mitra, and J. Heidemann, "Parametric methods for anomaly detection in aggregate traffic," IEEE/ACM Transactions on Networking (TON), vol. 19, pp. 512-525, 2011.

[13]. P. G. Bringas and Y. K. Penya, "Next-Generation Misuse and Anomaly Prevention System Enterprise Information Systems." vol. 19, J. Filipe and J. Cordeiro, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 117- 129.

[14]. X. D. Hoang, J. Hu, and P. Bertok, "A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference," Journal of Network and Computer Applications, vol. 32, pp. 1219- 1228, 2009.

[15]. H. T. Elshoush and I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey," Applied Soft Computing, vol. 11, pp. 4349-4365, 2011.

[16]. T. Pietraszek and A. Tanner, "Data mining and machine learning—Towards reducing false positives in intrusion detection," Information Security Technical Report, vol. 10, pp. 169-183, 2005.

[17]. S. Klüft, "Alarm management for intrusion detection systems - Prioritizing and presenting alarms from intrusion detection systems," Master, Computer Science Programme, Master of Science Thesis, University of Gothenburg, http://hdl.handle.net/2077/28856, 2012.

[18]. R. Lippmann, S. Webster, and D. Stetson, "The Effect of Identifying Vulnerabilities and Patching Software on the Utility of Network Intrusion Detection," in Recent Advances in Intrusion Detection. vol. 2516, A.

Wespi, G. Vigna, and L. Deri, Eds., ed: Springer Berlin / Heidelberg, 2002, pp. 307-326.

[19]. J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo, "Anomaly detection methods in wired networks: a survey and taxonomy," Computer Communications, vol. 27, pp. 1569-1584, 2004.

[20]. M. Leitner, P. Leitner, M. Zach, S. Collins, and C. Fahy, "Fault management based on peer-to-peer paradigms; a case study report from the celtic project madeira," in 10th IFIP/IEEE International Symposium on Integrated Network Management, pp. 697-700, 2007, pp. 697-700.

[21]. C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," Computers & Security, vol. 29, pp. 124-140, 2010.

[22]. A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, pp. 3448-3470, 2007.

[23]. R. Perdisci, G. Giacinto, and F. Roli, "Alarm clustering for intrusion detection systems in computer networks," Engineering Applications of Artificial Intelligence, vol. 19, pp. 429-438, 2006.

[24]. J. E. Gaffney Jr and J. W. Ulvila, "Evaluation of intrusion detectors: A decision theory approach," in IEEE Symposium on Security and Privacy, 2001. S&P 2001, Oakland, CA , USA. pp.50-61, 2001, pp. 50-61.

[25]. A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, "The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures," in Insider Attack and Cyber Security. vol. 39, S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, and S. Sinclair, Eds., ed: Springer US, 2008, pp. 17-52. [

[26]. P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, pp. 18-28, 2009.

[27]. G. M. Nazer and A. A. L. Selvakumar, "Current Intrusion Detection Techniques in Information Technology– A Detailed Analysis," European Journal of Scientific Research, vol. 65, pp. 611-624, 2011.

[28]. Nalla, Akash, and Anil Kumar Jakkani. "A Review on Recent Advances in Chatbot Design." integration 3.3 (2023).

[29]. S. Khanum, M. Usman, and A. Alwabel, "Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks," International Journal of Computer Science Issues, IJCSI, vol. 9, 2012.

[30]. O. Chung-Ming, "Host-based intrusion detection systems adapted from agent-based artificial immune systems," Neurocomputing, 2012.

[31]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[32]. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.

[33]. Y. Li, C. Jing, and J. Xu, "A New Distributed Intrusion Detection Method Based on Immune Mobile Agent Life System Modeling and Intelligent Computing." vol. 6328, K. Li, M. Fei, L. Jia, and G. Irwin, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 233-243.

[34]. O. Awodele, S. Idowu, O. Anjorin, and V. J. Joshua, "A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)," Issues in Informing Science and Information Technology, vol. 6, 2009.

[35]. Boozary, Payam. "The Impact of Marketing Automation on Consumer Buying Behavior in the Digital Space Via Artificial Intelligence." Power System Technology 48.1 (2024): 1008-1021.

[36]. Ayyalasomayajula et.al., Madan Mohan Tito. "A Cost-Effective Analysis of Machine Learning Workloads in Public Clouds: Is AutoML Always Worth Using?" International Journal of Computer Science Trends and Technology (IJCST), Oct. 2019.

[37]. Ayyalasomayajula et al., Madan Mohan Tito "Proactive Scaling Strategies for Cost-Efficient Hyperparameter Optimization in Cloud-Based Machine Learning Models: A Comprehensive Review." ESP Journal of Engineering & Technology Advancements, vol. 1, no. 2, 6 Dec. 2021, pp. 43-56.