Volume 9, Issue 6, June – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

Safeguarding Smart Horizons: Crafting the Future of IOT Security Through Intrusion Detection and Prevention

P. M. N. V. V. Sarveswara Gupta[1]; B. Venkateswarlu[2]; S. Karthikeya[3]; Dr. Mohan Kumar Chandol[4]; V. G. Sai Sumanth[5]
Computer Science and Engineering Koneru Lakshmaiah Educational Foundation, Guntur, India

Abstract:- It is crucial to secure digital assets and networks against harmful activity in the linked world of today. Through the detection and mitigation of unauthorized access, malicious activity, and possible security threats, Intrusion Detection and Prevention Systems (IDPS) are essential to the protection of systems and networks. The development, approaches, technologies, difficulties, and future directions of intrusion detection and prevention systems are all covered in detail in this research paper. The study examines the advantages and disadvantages of several IDPS methodologies, such as hybrid, anomaly-based, and signature-based techniques. It also addresses how to improve the efficacy and efficiency of IDPS using cutting-edge methods like big data analytics, artificial intelligence, and machine learning. In addition, the study discusses and suggests possible solutions for the problems that IDPS faces, including false positives, evasion strategies, and scalability concerns. In order to assist academics, researchers, and practitioners with insights, it concludes by outlining future directions for study and development in the field of intrusion detection and prevention systems.

Keywords:- *Intrusion Detection and Prevention Systems, IDPS, Signature-based, Anomaly-based, Machine Learning, Artificial Intelligence, Big Data Analytics.*

I. INTRODUCTION

With an increasing number of online hazards and interconnected systems in today's digital landscape, networks and sensitive data security has become critical for firms globally. As unwavering protectors against a variety of threats that persistently target networks with the intention of damaging security and integrity, intrusion detection and prevention systems, or IDPS, are indispensable. With its origins in the early years of networked computing, IDPS has evolved to mirror the never-ending game of cat and mouse between attackers and defenders. Strong and flexible defense systems are more important than ever as malevolent actors use more advanced techniques to breach networks and take advantage of weaknesses.

Driven by the necessity to safeguard vital resources and infrastructure, establishments have accepted IDPS as essential constituents of their cybersecurity armories. These systems are made to minimize the effects of security breaches by providing real-time monitoring and response capabilities in addition to being able to identify and block intrusion attempts. IDPS have made great strides in response to the dynamic threat landscape, utilizing state-of-the-art technology like artificial intelligence, machine learning, and big data analytics to improve their effectiveness and flexibility. But these improvements come with drawbacks as well: balancing false positive rates with detection precision, dealing with advanced adversaries' evasion tactics, and guaranteeing scalability to manage the increasing amount of network traffic.

This research paper endeavors to provide a comprehensive review of Intrusion Detection and Prevention Systems, delving into their evolution, methodologies, technologies, challenges, and future prospects. By synthesizing existing literature and analyzing contemporary trends, this paper aims to offer insights into the multifaceted landscape of IDPS, equipping readers with a nuanced understanding of their role in fortifying cybersecurity defenses. Through a structured exploration of the historical development, current landscape, and future directions of IDPS, this paper seeks to contribute to the ongoing discourse surrounding network security and resilience in the face of evolving cyber threats.

A. Background and Motivation:

IDPS originated in the early days of networked computing, when the internet was just getting started and faced its initial wave of cyberattacks. The threat landscape changed and technology progressed, making traditional security solutions ineffective against increasingly complex threats. Organizations turned to IDPS as a proactive defense mechanism because it was vital to protect sensitive data and key infrastructure.

B. Objectives:

The goal of this research study is to present a thorough overview of intrusion detection and prevention systems, covering their history, approaches, technologies, difficulties, and potential applications. Through a comprehensive review of the literature and an analysis of current trends, the study aims to:

- Follow the evolution of IDPS through its historical growth and key turning points.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

- Examine the several forms of IDPS and learn about their guiding concepts, approaches, and advantages over one another.
- Examine the technology and methods used in IDPS to help with detection and prevention.
- Examine the developments in IDPS, paying special attention to how big data analytics, artificial intelligence, and machine learning are integrated.
- Determine and discuss the obstacles and constraints that IDPS faces, and offer possible remedies and mitigating measures.
- Describe the planned paths for further study and advancement in the area of intrusion detection and prevention systems.

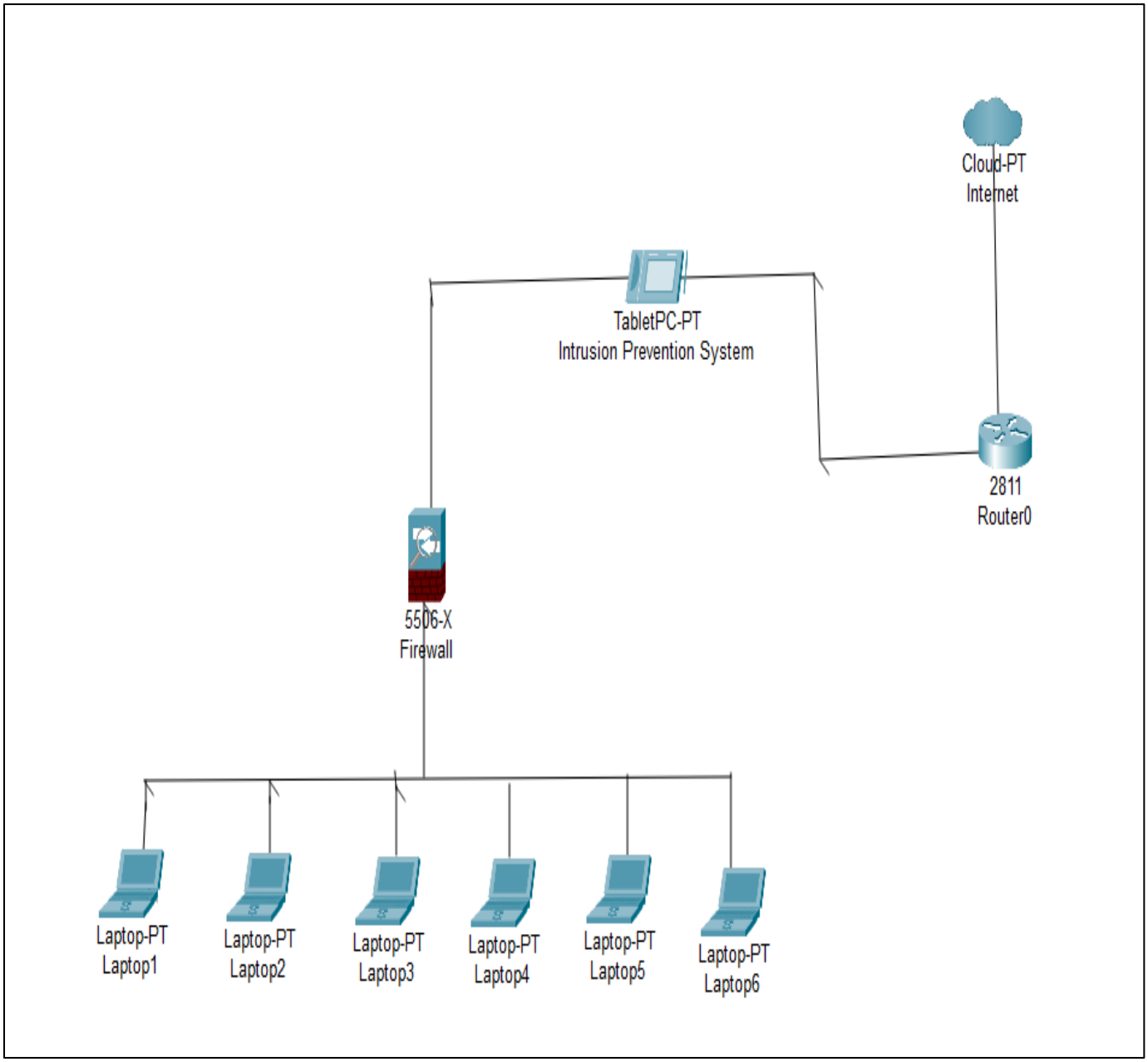

Fig 1: Intrusion Prevention System[1]

C. Scope and Organization of the Paper

This paper offers a methodical examination of IDPS, addressing a wide range of subjects crucial to comprehending their function in contemporary cybersecurity. The scope covers the historical development of IDPS, the different kinds and approaches used, technological improvements, difficulties encountered, and future directions. The paper's sections are each devoted to a distinct facet of IDPS, allowing readers to gain a thorough grasp.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

II. EVOLUTION OF INTRUSION DETECTION AND PREVENTION SYSTEMS

Of course! There are various significant phases in the evolution of intrusion detection and prevention systems (IDPS):

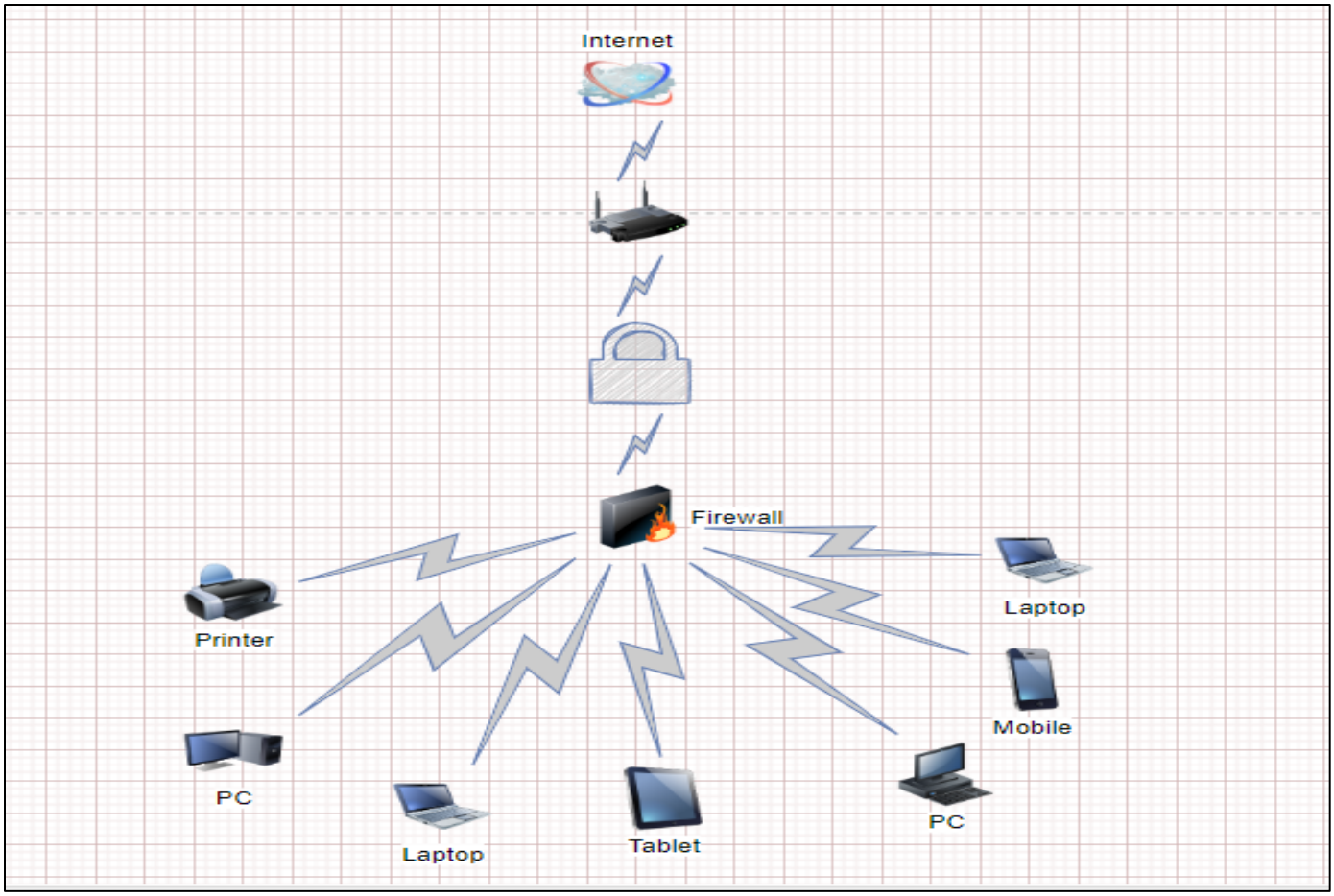

Fig 2: Evolution of Intrusion Detection and Prevention Systems[2]

A. Early Approaches (Pre-2000s):

When intrusion detection first emerged, its main objective was to identify network-based threats. During this period, important strategies included:

- Signature-Based Detection: This method of detection depends on patterns of malicious activity that have been identified. It does this by comparing system or network activity to a database of signatures, which are essentially pre-established patterns of recognized dangers. In order to identify known attacks, early intrusion detection systems (IDS) used signature-based detection; nevertheless, this method had limitations when it came to identifying unknown or novel threats.
- Anomaly-Based Detection: This method searches for behavioral abnormalities. It creates a baseline of typical system or network behavior and marks any variations from it as possibly malevolent or suspicious. Nevertheless, early anomaly detection systems were difficult to adjust for particular contexts and frequently had large false positive rates.

B. Transition to Modern IDPS (2000s - Early 2010s):

➢ *Intrusion Detection and Prevention Systems Developed to Meet these Issues as Cyber Threats Became More Complex:*

- Hybrid Approaches: To increase accuracy and coverage, many contemporary IDPS systems integrate anomaly- and signature-based detection methods. By utilizing anomalies to identify previously undiscovered attacks and signatures to identify known threats, hybrid approaches seek to combine the best features of both techniques.

- Behavior-Based Detection: Rather than emphasizing particular signs or anomalies, behavior-based detection looks for patterns of harmful conduct.

This method is examining a series of occurrences or acts to identify unusual activity that might point to a planned attack.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

A. Milestones and Significant Developments:

The evolution of IDPS has been shaped by several significant advancements and milestones.

The introduction of Intrusion Prevention Systems (IPS) was a reaction to the shortcomings of the conventional Intrusion Detection System (IDS). IPS has the ability to actively block or stop threats from reaching their targets, in contrast to IDS, which just detects and alerts.

IPS technologies helped enterprises more successfully reduce risks by introducing a crucial proactive layer to network security.

- AI and Machine Learning: The capabilities of IDPS have been greatly improved by the combination of AI and machine learning.

In order to improve detection accuracy and lower false positives, machine learning algorithms can scan enormous volumes of data to find patterns and anomalies that might point to hostile behavior.

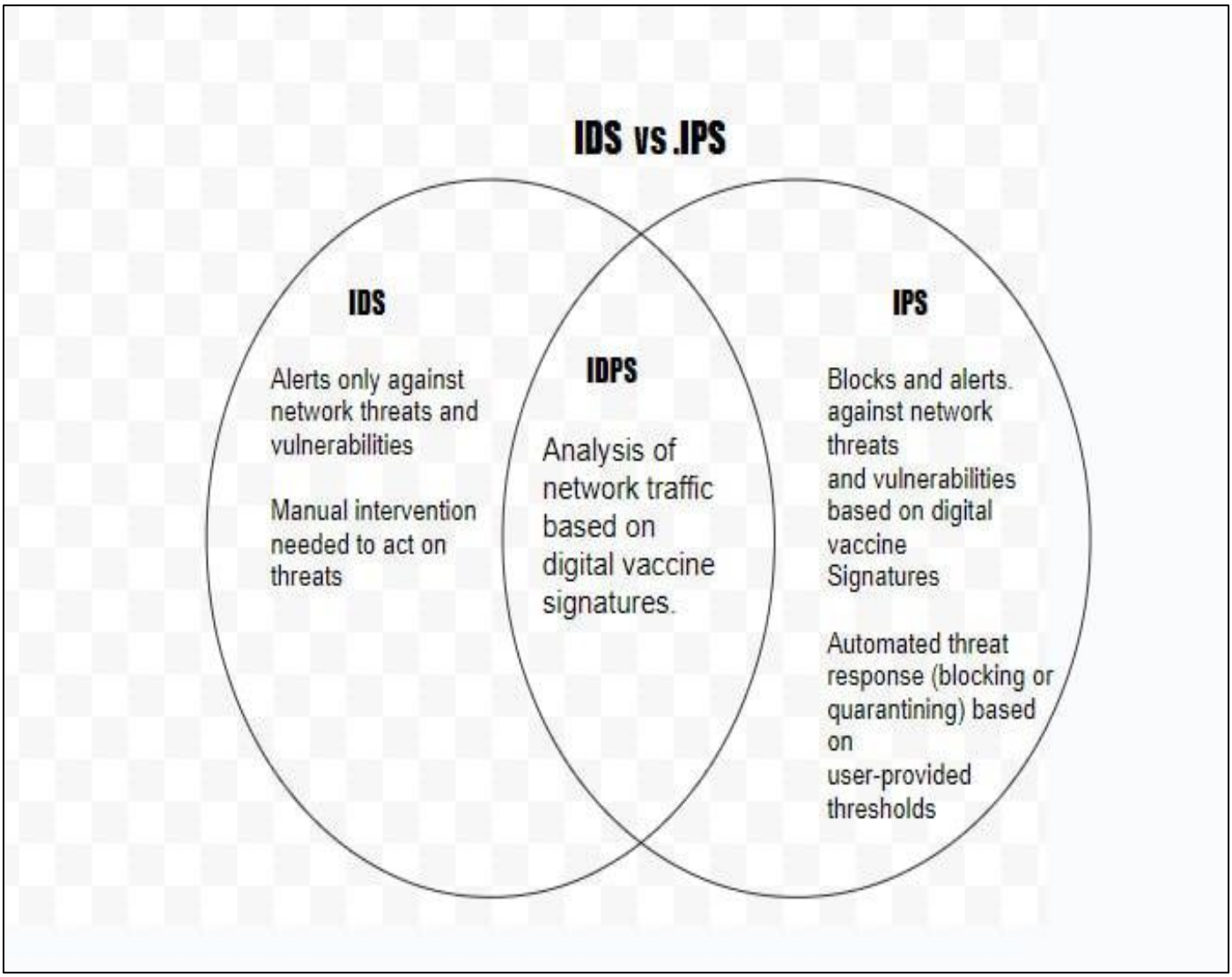

Fig 3: IDS vs IPS[3]

- Cloud-Based IDPS: IDPS systems have developed to offer cloud-native detection and prevention capabilities in response to the growth of cloud computing. Because it provides centralized management, scalability, and flexibility, cloud-based IDPS is a good fit for today's distributed and dynamic computing settings.
- Integration of Threat Intelligence: To improve detection capabilities, contemporary IDPS systems frequently interface with threat intelligence feeds. Through the use of current data regarding new threats and attack methods, IDPS is better equipped to recognize and address changing cybersecurity threats.

Overall, since security technologies continuously evolve to meet new threats and problems in the digital realm, IDPS's progress mirrors the ongoing arms race between cyber attackers and defenders.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

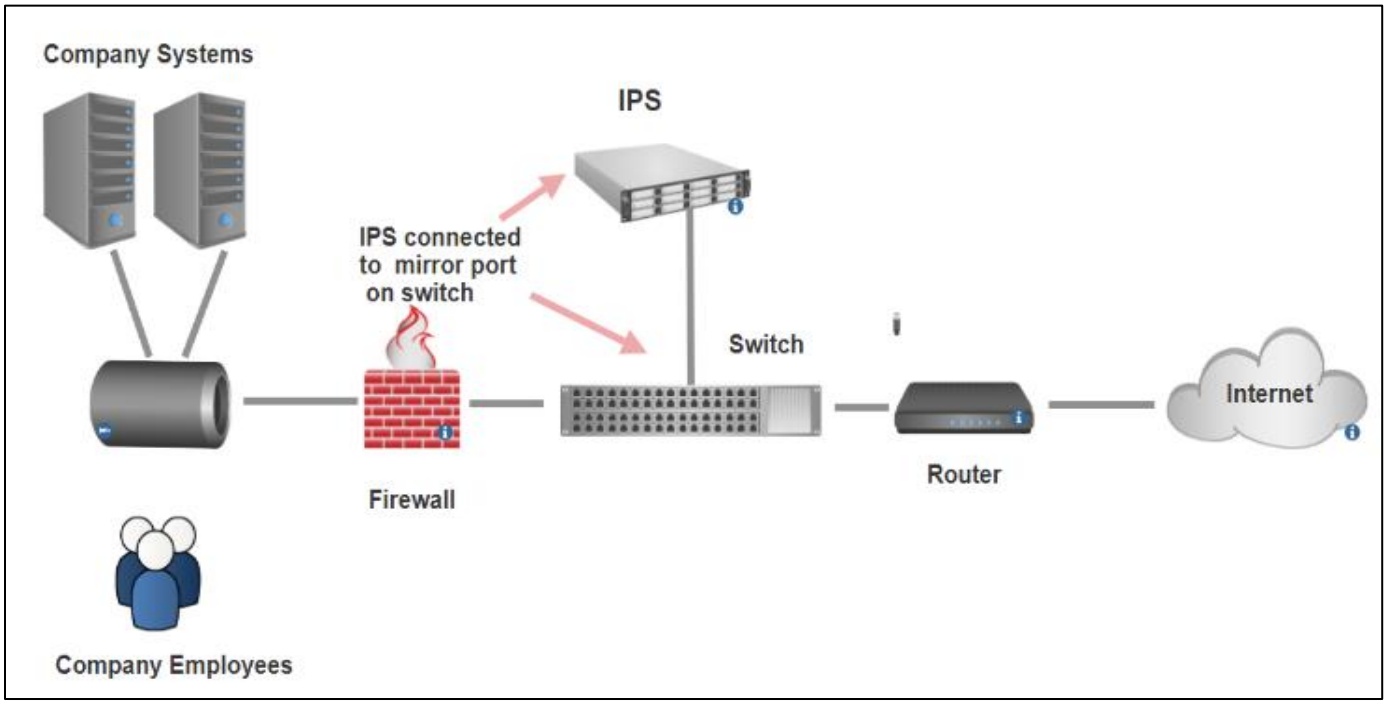

Fig 4: IDPS[4]

III. TYPES OF INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

A. Signature-based IDPS:

- Description: Signature-based intrusion detection and prevention systems, sometimes referred to as rule-based or pattern-matching detection, work by contrasting system activity or network traffic with a database of known attack signatures.
- Operation: By comparing data patterns with pre-defined signatures of known threats, it detects malicious behavior.
- Benefits: Excellent at accurately identifying known attacks. When compared to other techniques, it typically has less processing overhead.
- Restrictions: susceptible to known signature variants and zero-day attacks. If the attack signatures are not included in the database, it can produce false negatives.

B. Anomaly-based IDPS:

- An anomaly-based IDPS tracks network or system activity and detects departures from predetermined ranges of typical behavior.
- Operation: It creates a profile of typical behavior and marks any alterations as possibly suspicious.
- Benefits include the ability to identify new or unknown assaults. may change to meet new threats without needing regular upgrades.
- Limitations: prone to high false positive rates due to the possibility of flagging as suspicious legal activities that depart from the baseline. needs must be adjusted carefully to reduce false positives.

C. Hybrid Approaches:

Hybrid IDPS leverages the advantages of both signature-based and anomaly-based detection systems by combining them.

- Operation: To identify unknown or innovative assaults, it employs anomaly-based detection, while signature- based detection is used for recognized threats.
- Benefits: Provides better detection coverage and accuracy than single methods. can lessen the drawbacks of every technique.
- Limitations: The combination of several detection algorithms may lead to an increase in complexity. requires meticulous setup and adjustment to strike a balance between performance and detection accuracy.

D. Comparison and Evaluation:

- Anomaly-based vs. Signature-based: While anomaly-based IDPS can identify new threats but may generate more false positives, signature-based IDPS offers excellent accuracy for known threats but may overlook unidentified attacks.
- Hybrid vs. Individual Approaches: By combining the advantages of anomaly-based and signature-based techniques, hybrid approaches provide a balance between detection accuracy and coverage.

➢ *Criteria for Evaluation:*

- Effectiveness: The degree to which the IDPS is able to identify and stop incursions.
- False Positive Rate: The frequency with which benign behavior is mistakenly classified as malicious.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

- Scalability: The IDPS's capacity to manage rising traffic or activity quantities.
- Resource Utilization: The IDPS's resource requirements and computational overhead.
- Adaptability: The IDPS's capacity to adjust to changing network conditions and threats.

Organizations should take their unique security requirements, operational demands, and financial limits into account when choosing and assessing IDPS solutions in order to determine which approach—or approaches—is best. Regular testing and validation are also necessary to guarantee the efficiency and dependability of the selected IDPS solution.

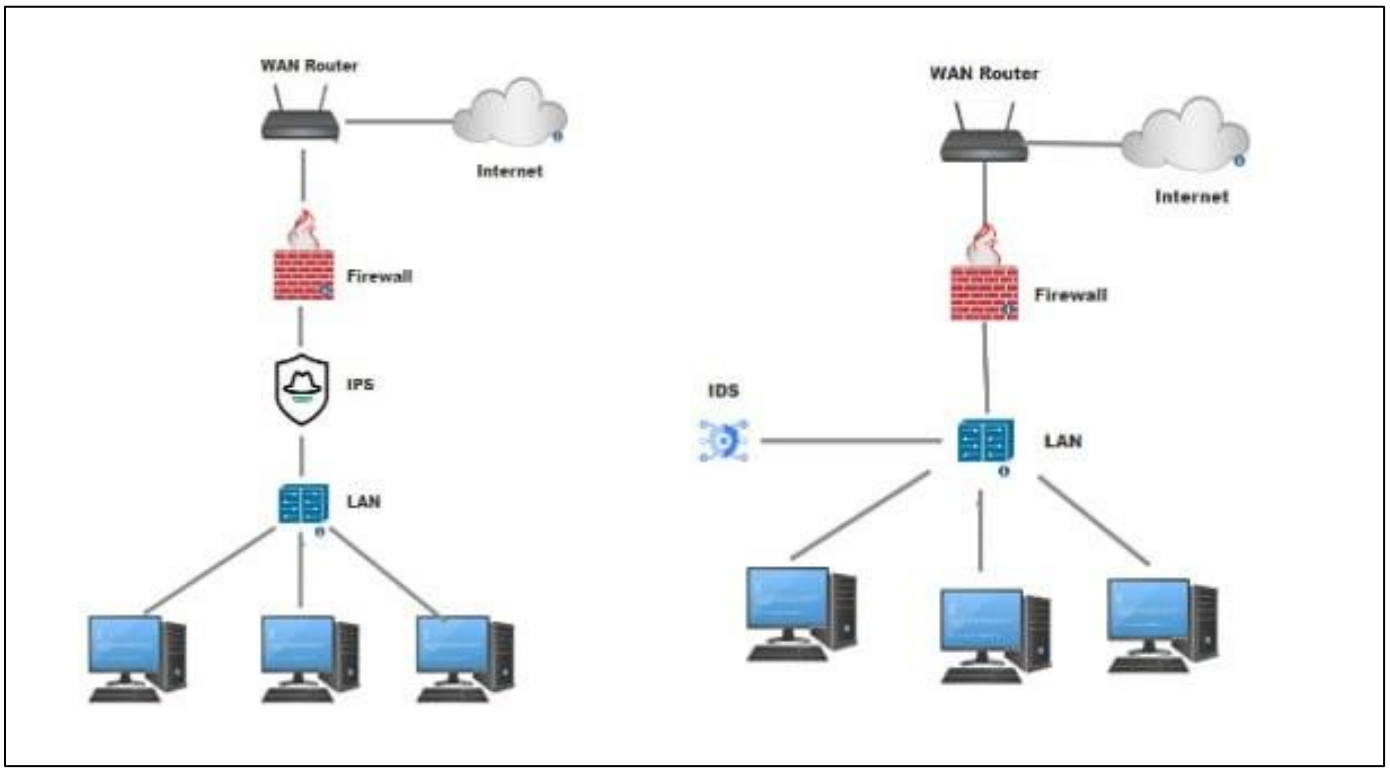

Fig 5: Intrusion Detection – Prevention Systems[5]

IV. METHODOLOGIES AND TECHNOLOGIES

A. *Detection Techniques:*

- Signature-based Detection: Synopsis: This method involves comparing system activity or network traffic to a database of recognized threat signatures.
- Operation: Compares data patterns to pre- defined threats' signatures.
- Benefits: Excellent at accurately identifying known attacks.
- Limitations: Open to known signature variants and zero-day attacks.

➢ *Analysis of Anomalies:*

- Description: Keeps an eye on network or system activity and spots departures from predetermined norms of acceptable conduct.
- Operation: Creates a baseline of typical conduct and marks any variations as possibly suspicious.
- Benefits: Can identify new or unidentified assaults without depending on pre-established signatures.
- Limitations: Needs careful tuning and is prone to high false positive rates.

➢ *Conduct-oriented Detection:*

- Description: Rather to concentrating on particular signatures or abnormalities, this approach identifies patterns of malicious behavior.
- Operation: Examines a series of events or acts to look for unusual activity.
- Benefits: Able to identify complex attacks that sidestep approaches based on signatures and anomalies.
- Limitations: Needs sophisticated analytics and, if improperly configured, could result in false positives.

B. *Prevention Mechanisms:*

➢ *IDPS Uses Prevention Strategies to Actively Prevent or Lessen Dangers that are Detected.*

- Intrusion Prevention Systems (IPS): Described as actively stopping or preventing recognized threats from reaching their objectives, IPS extends the capabilities of intrusion detection.
- Operation: Examines system or network activity and takes appropriate steps to stop or quarantine malicious behavior.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

- Benefits: Prevents security problems before they have a chance to cause harm.
- Restrictions: It needs to be carefully configured to prevent interfering with valid communications and may produce false positives.
- Packet filtering: Describes: Applys pre- established rules or criteria to filter incoming and outgoing network traffic.
- Operation: Examines packets, deciding whether to accept or reject them based on predetermined standards such protocol, source IP, and destination IP.
- Benefits: Offers a fundamental degree of defense against known dangers and illegal entry.
- Restrictions: Its capacity to identify and stop complex attacks is limited.

C. Integration with Security Frameworks:

To improve overall cybersecurity posture, IDPS can be linked with larger security frameworks:

➢ *Security Information and Event Management (SIEM):*

The purpose of Security Information and Event Management (SIEM) is to provide comprehensive threat detection and response capabilities by gathering and analyzing security event data from several sources, such as IDPS.

- Operation: Linking events from several sources together allows you to prioritize your response activities and spot possible security incidents.
- Benefits: Enhances visibility and collaboration by centralizing security monitoring and administration.
- Limitations: To successfully correlate and evaluate security events, careful configuration and tuning are needed.
- Integration of Threat Intelligence: Synopsis: This feature enhances detection capabilities by integrating with threat intelligence feeds and furnishes prompt alerts on new threats.
- Operation: Updates detection and prevention procedures with current knowledge about known threats and attack methods.
- Benefits: Increases the accuracy of detection and permits proactive defense against changing threats.
- Limitations: Dependent on threat intelligence streams' timeliness and quality.

By integrating with security frameworks, IDPS is able to better utilize additional information and intelligence sources to enhance its capabilities for threat detection and response. Organizations can create resilient defense-in-depth strategies that are adaptable to a variety of cybersecurity threats by integrating detection techniques, prevention mechanisms, and integration with security frameworks.

V. ADVANCEMENTS IN INTRUSION DETECTION AND PREVENTION SYSTEMS

A. Machine Learning Techniques:

IDPS has undergone a revolution thanks to machine learning (ML) techniques, which allow systems to learn from data and gradually enhance their detection capabilities:

- Large data sets are analyzed by machine learning algorithms to find patterns and abnormalities that point to possible hostile behavior.
- Applications: Both signature-based and anomaly-based detection techniques make use of machine learning. Based on observed trends, it may automatically create and update signatures and adjust to changing threats.
- Benefits: ML lowers false positive rates and strengthens overall security posture by enabling IDPS to detect sophisticated and hitherto undetected attacks with high accuracy.
- Difficulties: ML models can be vulnerable to evasion tactics used by skilled attackers and necessitate big and diverse datasets for training.

B. Artificial Intelligence Applications:

IDPS capabilities are improved by artificial intelligence (AI) approaches, which provide systems the ability to decide for themselves and act accordingly:

- Artificial Intelligence (AI) comprises diverse methodologies, including machine learning, natural language processing, and expert systems.
- Applications: In real time, AI-powered IDPS can independently identify, evaluate, and react to security risks. They may also adjust to shifting settings and automate incident response procedures.
- Benefits: IDPS can scale and react quickly to threats thanks to AI, which lessens the workload for human analysts and boosts overall effectiveness.
- Challenges: It may be difficult to comprehend AI systems' decision-making processes because to their lack of interpretability and transparency. Strong cybersecurity measures are also necessary to defend against hostile attacks.

C. Big Data Analytics:

IDPS can efficiently process and analyze large amounts of data thanks to big data analytics technologies:

- IDPS can now ingest, store, and analyze massive amounts of security event data from a variety of sources thanks to big data analytics platforms.
- Applications: IDPS can correlate security events, find intricate attack patterns, and quickly discover new threats by utilizing big data analytics.
- Benefits: By enhancing IDPS's visibility into network and system activity using big data analytics, more precise threat detection and response are made possible.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

- Challenges: Robust infrastructure and computational resources are necessary for managing and analyzing massive datasets. Furthermore, it's critical to guarantee data protection and regulatory compliance.

D. Blockchain and Cryptographic Solutions:

The security and integrity of IDPS data and processes are improved by blockchain technology and cryptographic solutions:

- To record security events and transactions, blockchain technology offers a decentralized, impenetrable ledger. Digital signatures and encryption are two examples of cryptographic techniques that guarantee the secrecy, integrity, and validity of data.
- Applications: IDPS may exchange threat intelligence, safely store audit records, and verify the accuracy of security event data using blockchain technology. Within IDPS, cryptography can safeguard private data and communication routes.
- Benefits: IDPS data is more dependable and trustworthy thanks to blockchain technology and cryptographic solutions, which also reduce the possibility of data manipulation and illegal access.
- Difficulties: Careful planning and interaction with the current IDPS infrastructure are necessary for the implementation of blockchain and cryptography solutions. Furthermore, keeping cryptographic keys and making sure that appropriate key management procedures are followed are crucial for security.

In general, IDPS capabilities are changing as a result of developments in machine learning, artificial intelligence, big data analytics, blockchain, and cryptography. This helps enterprises identify, stop, and respond to cybersecurity threats more successfully in the ever-changing threat landscape of today.

VI. CHALLENGES AND LIMITATIONS

It is imperative to tackle obstacles and constraints in order to guarantee the efficiency and dependability of Intrusion Detection and Prevention Systems (IDPS). Here are a few of the main obstacles and constraints that IDPS has to deal with:

A. False Positives and Negatives:

- False Positives: When acceptable actions are mistakenly reported by IDPS as malicious, this might result in needless alarms and possibly impair regular operations.
- False Negatives: When IDPS is unable to identify real security risks, hostile activity may continue undetected and lead to security lapses.
- Mitigation: You can lessen false positives and negatives by fine-tuning detection thresholds, utilizing a variety of detection methods, and putting in place thorough validation procedures.

B. Evasion Techniques:

- Evasion Techniques: To avoid IDPS detection, skilled attackers may use evasion techniques like encryption, obfuscation, fragmentation, and protocol manipulation.
- Evasion efforts can be lessened by deploying intrusion prevention systems, doing deep packet inspection, and routinely updating detection algorithms to take into account new evasion strategies.

C. Scalability Issues:

- Scalability: As network traffic quantities rise, IDPS may find it more difficult to handle and analyze data instantly, which could result in a drop in performance and possible gaps in detection coverage.
- Mitigation: To improve scalability and handle increasing traffic volumes, distributed IDPS systems, cloud-based solutions, and parallel processing can be used to optimize resource use.

D. Privacy Concerns:

- Privacy Concerns: IDPS involves monitoring and analyzing network and system activity, raising concerns about privacy, data confidentiality, and compliance with regulations such as GDPR.
- Mitigation: Implementing privacy-preserving techniques such as data anonymization and encryption, defining clear data retention and access policies, and conducting regular privacy impact assessments can address privacy concerns and ensure compliance with regulations.

E. Operational Overhead:

- Operational Overhead: It takes a lot of time, money, and experience to manage and maintain IDPS systems. It might take a lot of work to configure, adjust, and update detection algorithms and signatures.
- Mitigation: Reducing operational overhead and increasing efficiency can be achieved by investing in automation technologies for configuration management, utilizing managed security services, and giving security staff continual training.

F. Adapting to Evolving Threat Landscape:

- Changing Threat Environment: methods, and procedures (TTPs).
- Mitigation: To stay ahead of evolving threats, IDPS can use tools like threat intelligence feeds, regular threat hunting exIn order to avoid IDPS detection, attackers a re-always creating new tactics, mercises, and industry peer collaboration to share best practices and insights.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

A multifaceted strategy combining technical fixes, operational procedures, and continuing cooperation between security teams, vendors, and industry partners is needed to address these obstacles and restrictions. Organizations can improve their overall cybersecurity posture and optimize the efficiency of their IDPS by taking proactive measures to solve these issues.

VII. FUTURE DIRECTIONS

The development of intrusion detection and prevention systems (IDPS) is anticipated to be shaped by a number of significant trends and directions in the future:

A. Enhanced Threat Intelligence Integration:

- Description: To improve detection capabilities and offer timely insights into new threats, IDPS will increasingly interact with advanced threat intelligence feeds and platforms.
- Benefits: By proactively identifying and responding to developing threats, enhanced threat intelligence integration will help IDPS improve overall security posture and resilience.
- Applications: Real-time threat analysis, automated incident response, and dynamic rule modification based on threat intelligence feeds will be made easier by integration with threat intelligence platforms.

B. Contextual Awareness and Adaptability:

- Description: In order to better comprehend the distinctive qualities of the environment they safeguard, future IDPS systems will make use of contextual awareness and adaptive capabilities.
- Benefits: By enhancing detection accuracy and decreasing false positives, contextual awareness will help IDPS distinguish between normal and deviant behavior.
- Applications: To customize detection rules and reaction actions to certain scenarios, IDPS will take into account contextual data such as user behavior, device type, location, and business processes.

C. Automation and Orchestration:

- IDPS will increasingly rely on automation and orchestration capabilities to enable prompt and well-coordinated responses to security issues.
- Benefits: Automation will lighten the strain for security professionals, expedite threat detection and mitigation, and streamline incident response procedures.
- Applications: IDPS will use automation and orchestration to implement remedial activities, update security policies in real-time, quarantine compromised systems, and automatically analyze alerts.

D. Quantum Computing Implications:

The advent of quantum computing presents IDPS with potential advantages and disadvantages, as its capabilities could make current encryption techniques outdated.

- Challenges: The secrecy, integrity, and validity of IDPS data and communications may be jeopardized by the possibility that quantum computing will defeat widely used encryption techniques.
- Possibilities: In order to protect IDPS in the post-quantum age from assaults by quantum computers, quantum-safe cryptography algorithms and methods are being developed.

IDPS providers and organizations must update cryptographic protocols, implement quantum- safe cryptography, and make sure their security architecture is resilient in order to be ready for the era of quantum computing.

To sum up, improved threat intelligence integration, contextual awareness, automation and orchestration, and quantum computing readiness will define the future of IDPS. Organizations may fortify their cybersecurity defenses and successfully counter new threats in a dynamic threat landscape by adopting these future trends.

VIII. RESULT AND ANALYSIS

A. Summary:

- Enhanced Threat Intelligence Integration: To strengthen detection skills and better address changing threats, IDPS will interface with advanced threat intelligence feeds and platforms.
- Contextual Awareness and Adaptability: In order to better comprehend the environment they guard, future IDPS systems will make use of contextual data. This will improve threat detection accuracy and decrease false positives.
- Automation and Orchestration: By streamlining incident response procedures, automation and orchestration capabilities will allow for quick and coordinated action to reduce security occurrences.
- Implications of Quantum Computing: To maintain security in the post-quantum future, IDPS must prepare for quantum-safe cryptography, which poses both opportunities and challenges.

B. Analysis:

- Benefits: Adopting these future directions can improve IDPS's overall cybersecurity posture, threat detection, reaction times, and efficacy and resilience.
- Challenges: Considerable expenditures in infrastructure, knowledge, and technology may be necessary to implement contextual awareness, automation capabilities, and sophisticated threat intelligence integration.

- Possibilities: Organizations may fortify their defenses against changing cyberthreats and preserve a competitive edge in the digital market by keeping ahead of developing technology and threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN2043

Organizations must proactively prepare for the future by making investments in R&D, revising existing security plans, and working with business partners to take advantage of new opportunities and challenges.

In conclusion, IDPS has a bright future ahead of it for improving cybersecurity capabilities, but there are obstacles along the way that will need to be carefully considered, moneyed for, and conquered in order to succeed. Organizations can successfully safeguard their assets and uphold confidence in the digital era by adopting these future paths and remaining watchful in the face of changing dangers.

IX. CONCLUSION

To sum up, there have been notable developments in detection methods, defense mechanisms, and security framework integration over the life of intrusion detection and prevention systems (IDPS). IDPS has continuously changed to meet changing cyber threats, starting with early signature-based methods and continuing with contemporary machine learning and artificial intelligence applications.

IDPS has a bright future ahead of it, with potential for improved automation, contextual awareness, threat intelligence integration, and quantum computing implications. Organizations can strengthen their cybersecurity defenses, enhance their threat detection and response capabilities, and maintain their resilience in the face of new threats by adopting these future directions.

To fully utilize IDPS, however, a number of obstacles need to be overcome, including false positives and negatives, evasion strategies, scalability problems, privacy issues, and the implications of quantum computing. Proactive action, investments in knowledge and technology, and cooperation amongst many industry sectors are needed for this.

Fundamentally, IDPS's future depends on its capacity to adjust to shifting threat environments, make efficient use of cutting-edge technology, and work with others to stay ahead of new cyberthreats. Organizations can effectively traverse the complicated landscape of cybersecurity and protect their digital assets in an increasingly interconnected world by placing a high priority on innovation, resilience, and collaboration.

REFERENCES

[1]. Anderson, D. (2019). Intrusion Detection and Prevention Systems: Concepts and Techniques (Advances in Information Security, Privacy, and Ethics). IGI Global.
[2]. Kent, K. (2018). Network Intrusion Detection and Prevention: Concepts and Techniques. Springer.
[3]. A. Gendreau and M. Moorman, “Survey of intrusion detection systems towards an end to end secure internet of things,” in Proceedings of the 4th IEEE International Conference on Future Internet of Things and Cloud (FiCloud '16), pp. 84–90, IEEE Computer, Vienna, Austria, August 2016.
[4]. M. Ammar, G. Russello, and B. Crispo, “Internet of Things: a survey on the security of IoT frameworks,” Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
[5]. F. Restuccia, S. D'Oro, and T. Melodia, “Securing the internet of things in the age of machine learning and software-defined networking,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829–4842, 2018.
[6]. Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. In Proceedings of the 13th USENIX Conference on System Administration (Vol. 13, pp. 229-238).
[7]. Shin, S., Gu, G., Porras, P., Yegneswaran, V., & Fong, M. (2011). Avant-Guard: Scalable and Vigilant Switch Flow Management in Software-Defined Networks. In Proceedings of the 2011 ACM SIGCOMM Conference (pp. 408-409).
[8]. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). Alert Verification in Intrusion Detection Systems. ACM Transactions on Information and System Security, 7(4), 585-615.
[9]. Moore, A. W., & Edsall, T. (2003). A Social Network Analysis of IRC Botnets. In Proceedings of the 3rd Usenix Steps to Reducing Unwanted Traffic on the Internet Workshop (pp. 91-98).
[10]. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan, “Trust management techniques for the internet of things: a survey,” IEEE Access, vol. 7, pp. 29763–29787, 2019.
[11]. Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, “A global hybrid intrusion detection system for wireless sensor networks,” Procedia Computer Science, vol. 52, pp. 1047–1052, 2015.
[12]. S. M. Sajjad, S. H. Bouk, and M. Yousaf, “Neighbor node trust based intrusion detection system for WSN,” Procedia Computer Science, vol. 63, pp. 183–188, 2015.
[13]. E. M. Shakshuki, N. Kang, and T. R. Sheltami, “EAACK — a secure intrusion-detection system for MANETs,” IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089–1098, 2013.
[14]. J. Bhar, “A mac protocol implementation for wireless sensor network,” Journal of Computer Networks and Communications, vol. 2015, no. 1, 2015.
[15]. Jung, J., & McHugh, J. (2001). Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context. In Proceedings of the 10th USENIX Security Symposium (Vol. 10, pp. 207-220).
[16]. Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in Computing (3rd ed.). Prentice Hall.
[17]. Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.
[18]. Dittrich, D., & Kennington, J. (2001). Threats and Vulnerabilities in Distributed Systems. IEEE Security & Privacy, 1(6), 66-73.