RESEARCH ARTICLE OPEN ACCESS

A Comprehensive review of IoT applications, security issues, and intrusion detection strategies

Dr. Amina Vali
Department of Science and Technology (Sadabai Raisoni Women's College Nagpur) (SNDT University ,Mumbai)

Dr. Rozina Naz
department of Science and Technology (Sadabai Raisoni Women's College,Nagpur) (SNDT University, Mumbai)

Mr. Noorul Amin
department of Science and Technology (Sadabai Raisoni Women's College, Nagpur) (SNDT University, Mumbai)

***Abstract*— The Internet of Things (IoT) is rapidly expanding and integrating into various aspects of daily life, including education, homes, transportation, and healthcare. However, as the number of connected devices grows, so do the associated challenges, such as heterogeneity, scalability, quality of service, and security concerns. Due to limitations in cost, size, and power, security management is often overlooked, increasing the risk of cyber threats. This lack of security discourages users from adopting IoT devices and exposes them to financial and reputational risks. This study provides an in-depth analysis of security challenges across different IoT layers, including the perception, network, support, and application layers. It also offers an in-depth analysis of the latest Intrusion Detection System (IDS) methods, emphasizing significant vulnerabilities and examining potential improvements in security. The findings emphasize the importance of strengthening IoT security to ensure safer and more reliable connected environments.**

Keywords— IoT, IDS, scalability, heterogeneity, security

I. INTRODUCTION

IoT is a growing field enabling data collection and transfer without human intervention. It connects objects with sensors, software, and control systems, evolving through advances like machine learning[1]. IoT applications are becoming more prevalent across various sectors. A few of the most common uses of IoT are illustrated in Figure 1.

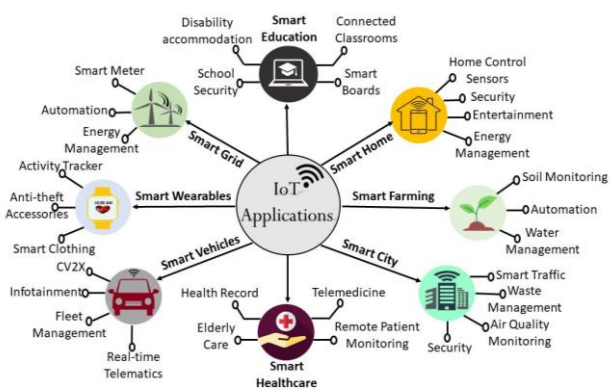

Figure 1. A representation of various IoT applications[1].

Connectivity is being adopted across all sectors, including education, where IoT supports students with disabilities. In smart homes and cities, IoT enhances safety, waste disposal systems, air quality, and entertainment experiences. [2]. The healthcare industry has been revolutionized by the advent of IoT, including innovations like devices worn on the body, telehealth services, and remote monitoring of patients. [3]. IoT has transformed traditional farming practices in agriculture, facilitating better management of water resources and monitoring of soil conditions [4]. The automotive industry has been transformed by IoT, allowing for the creation of connected vehicles [5]. Additionally, the integration of IoT in electric grids has elevated energy management to new levels [6]. IoT has grown into a vast industry through numerous advancements, with its progress over time illustrated in Fig. 2. It has evolved from internet-enabled refrigerators to IoT-powered smart cities [7]. The industry has made significant progress and has become a vital aspect of everyday living. IoT made its way into defense by following the launch of the Internet of Battlefields in 2017 and its expansion into healthcare in 2018. In 2005, Japan launched the first Wi-Fi-enabled rabbit. [8]. In 2011, IoT was featured in the Hype Cycle for emerging technologies and reached its peak in Gartner's cycle by 2017. [9]. After the widespread IoT-based attack in 2016, the emphasis has now moved to IoT security [10].

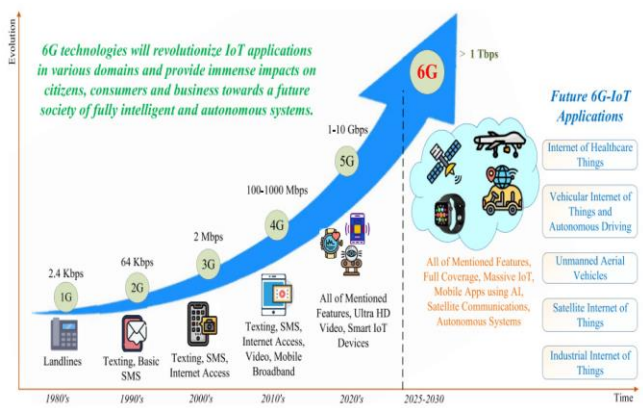

Fig 2: Figure 2 A timeline illustrating the development of IoT technologies from 1980 to 2030[1].

Figure 3. A visual depiction of the different research challenges in IoT[1].

Figure 3 highlights IoT research challenges, including non-unified security protocols, heterogeneous devices, and

lack of standardization. Traditional security methods are impractical due to limited processing power. Security is further constrained by power, location, and mobility, especially in smart automobiles [11]. Building trust is more straightforward in stationary IoT applications compared to those in fast-moving vehicles. IoT faces resource constraints like cost, power, and size, while device heterogeneity remains a challenge in distributed environments [12].

Table I: IoT research challenges.

Title	Author(s)	Year	Research Challenges	Discussion
IoT Standardization: The Road Ahead	A. Pal, H. K. Rath, S. Shailendra, A. Bhattacharyya	2018	Lack of standardization, interoperability issues	Discusses the need for global IoT standards and challenges in achieving them
Future IoT-enabled Threats and Vulnerabilities: State of the Art, Challenges, and Future Prospects	A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, V. J. Aski	2020	Security threats, privacy concerns, scalability	Examines current and emerging IoT vulnerabilities and suggests mitigation strategies
IoT Connectivity Technologies and Applications: A Survey	J. Ding, M. Nemati, C. Ranaweera, J. Choi	2020	Connectivity limitations, power constraints, scalability	Surveys various IoT connectivity technologies and their applications
Secure, Sustainable Smart Cities and the Internet of Things	I. Hussain	2024	Cybersecurity risks, sustainability challenges	Explores IoT applications in smart cities and discusses security and sustainability issues
A Holistic Analysis of IoT Security: Principles, Practices, and New Perspectives	M. Hossain, G. Kayas, R. Hasan, A. Skjellum, S. Noor, S. R. Islam	2024	Security principles, attack mitigation, privacy concerns	Provides an extensive review of IoT security practices and new perspectives
The Internet of Things: Security Challenges and Opportunities	P. Baniya, A. Agrawal, K. Abid, J. Nath, B. K. Chaudhary, B. Kunwar	2024	Authentication, encryption, data integrity	Discusses IoT security threats and potential opportunities for improvement
Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions	M. Adil, M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani, Z. Jin	2024	Patient data security, privacy issues, device vulnerabilities	Focuses on security threats in healthcare IoT and proposes future research directions

IoT Security in a Connected World: Analyzing Threats, Vulnerabilities, and Mitigation Strategies	M. R. Tawffaq, M. A. Jasim, B. G. Mejbel, S. S. Issa, L. Alamro, V. Shulha, E. Aram	2024	Threats, vulnerabilities, mitigation techniques	Analyzes security challenges in IoT and suggests mitigation strategies

Interoperability is also crucial as the number of connected devices grows, yet common platforms for IoT remain limited. Connectivity becomes a major concern, especially with the inclusion of essential IoT devices in data transmission. Guaranteeing consistent data transfer between various IoT devices is a major technical challenge. Security is vital for maintaining consumer trust in IoT systems, but security management often takes a lower priority due to factors such as cost, size, and power consumption. This oversight leaves IoT systems vulnerable to security breaches, which can result in substantial financial and reputational damage.

Research Contributions: Numerous surveys are available in the literature, with Table 1 summarizing the main contributions of some of the most frequently referenced studies. This work provides an overview, starting with the evolution and applications of IoT. The study begins by addressing security challenges across various layers and concludes with an examination of different Intrusion Detection methods. The primary focus of this research is on tackling the security concerns related to IoT technology. Key contributions of the study include:

- An overview of the evolution of IoT, its applications, and the associated challenges.
- A focused discussion on security issues at different IoT layers.
- A comprehensive review of recent Intrusion Detection System techniques.

II. SECURITY CHALLENGES IN THE IOT DOMAIN

The number of Internet of Things (IoT) devices is rapidly increasing, and the absence of proper security measures has turned these devices into a target for malicious activities [24].

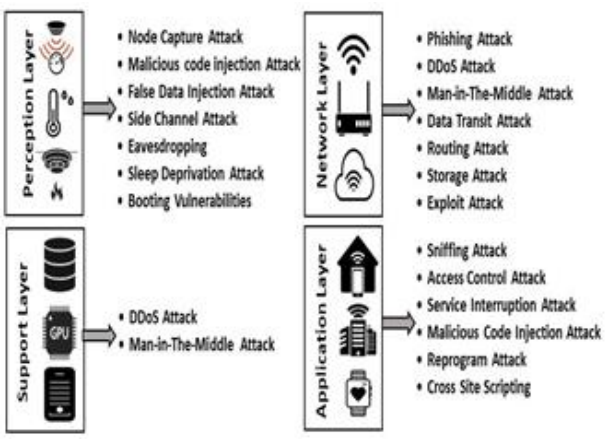

Figure 4: A visual depiction of various security attacks across different layers of IoT[2].

Figure 4 illustrates different cybersecurity attacks that can affect various IoT layers, including the Perception layer, Support layer, Network layer, and Application layer. The review work adopts a widely recognized four-layered design for analysis [21].

A. PERCEPTION LAYER

The perception layer consists of sensors and actuators.[22]. Sensors collect data from their surroundings, while actuators respond by taking actions derived from that data, sensors, also referred to as nodes are vulnerable to attacks where hackers can capture or replace them with malicious ones. Updating their software wirelessly can also enable attackers to introduce malicious or incorrect data, resulting in security vulnerabilities [23]. This layer is vulnerable to side-channel attacks, which may involve laser, power consumption, or timing-based methods [24]. Nodes in open environments are susceptible to eavesdropping attacks during data transmission or similar activities [25]. IoT gadgets have limited power resources, and cybercriminals can deplete their battery, leading to operational downtime. Since security only starts after booting, attackers can target the device during startup.

B. NETWORK LAYER

The network layer transmits data from the detection layer to the processing unit for further processing. This layer is particularly susceptible to attacks, given the involvement of multiple IoT devices [26]. A phishing attack aims at multiple IoT devices with the goal of gaining control over some of them [27]. In a DDoS attack, the attacker seeks to overwhelm the target by sending deceptive requests. IoT devices act as botnets in these attacks, producing a massive amount of requests that can block the target from accessing its resources [28]. Worm-hole and Sinkhole attacks are forms of routing-based attacks where the attacker gains control of nodes to redirect traffic along an alternate path [29].

C. SUPPORT LAYER

The Support layer functions between the Network and Application layers, enabling tasks like resource management, computation, and data storage. Protecting the database is essential at this layer, as it is susceptible to attacks such as DDoS, Man-in-the-Middle, and SQL injection. Communication between clients and service providers is typically handled by a broker, such as the MQTT protocol. In a Man-in-the-Middle attack, the attacker intercepts and manipulates the communication between the broker and the involved parties, thereby intercepting and manipulating all communication [30]. In the Support layer,

the primary target of attacks is often data access, making the security of databases and cloud systems vital at this layer.

D. APPLICATION LAYER

The application layer includes intelligent applications such as smart cities, smart homes, healthcare, and others. Since this layer interacts directly with end-users, privacy and data theft are significant concerns [31]. This layer faces malicious code injection and service interruption attacks, like denial of service. Compromised privileged access can lead to system-wide breaches, making access control a major concern[32]. A sniffing attack occurs when an attacker uses sniffing tools to capture network traffic, potentially compromising sensitive data in the process [33].

III. INTRUSION DETECTION SYSTEM

As we move into an age where almost every device humans use is connected to the internet, securing these devices becomes essential. Two key solutions for preventing DDoS attacks identified in the literature are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). IDS serves as a precautionary tool, raising an alarm when an intrusion occurs but taking no direct action. In contrast, IPS is a more proactive approach, where the system takes action in response to an intrusion [34]. In an IPS, false positives are a significant issue, as they may result in blocking legitimate users. Table 2 presents a comprehensive comparative analysis of IDS and IPS systems. This research primarily focuses on IDS, due to the concern over false alarm rates in malware classification. Moreover, penalizing legitimate users undermines the effectiveness of a detection system. Figure 6 illustrates the different categories of Intrusion Detection Systems (IDS). Depending on the target location, IDS can be classified into Host-based, Network-based, or Hybrid types. Host-based IDS is designed for individual systems, making it effective for detecting internal intruders and evaluating the scope of a compromise, but it is costly as a separate IDS is needed for each host[35]. In Network-based IDS, external intrusions are detected efficiently, and it can safeguard all hosts; however, the main challenge is managing and analyzing the large volume of traffic [36]. Hybrid IDS offers greater flexibility and enhanced security by combining the features of both Host-based and Network-based IDS [37]. In Active IDS, specific actions are taken in response to certain alerts, while Passive IDS only generates reports or raises alarms. Centralized IDS uses individual monitors to track each host, but it lacks scalability and flexibility, making it less adaptable to varying requirements. Additionally, centralized IDS is vulnerable to a single point of failure. In contrast, Distributed IDS operates on a Peer-to-Peer (P2P) architecture, where each monitoring unit also serves as an analysis unit.

Table II: Comparative analysis of IDS And IPS systems.

Feature	**Intrusion Detection System (IDS)**	**Intrusion Prevention System (IPS)**
Function	Monitors and detects suspicious activity	Detects and actively blocks threats
Response	Alerts administrators	Prevents attacks in real-time
Placement	Typically placed within the network to monitor traffic	Positioned inline to control and filter traffic
Action Taken	Logs and reports incidents	Blocks, modifies, or redirects malicious traffic
Effect on Network	Minimal impact on traffic flow	Can introduce latency due to traffic filtering
False Positives	May generate alerts for benign activities	Can sometimes block legitimate traffic
Security Level	Passive approach, does not stop attacks	Active approach, prevents attacks from occurring
Usage Scenario	Suitable for monitoring and forensic analysis	Best for proactive security and real-time protection

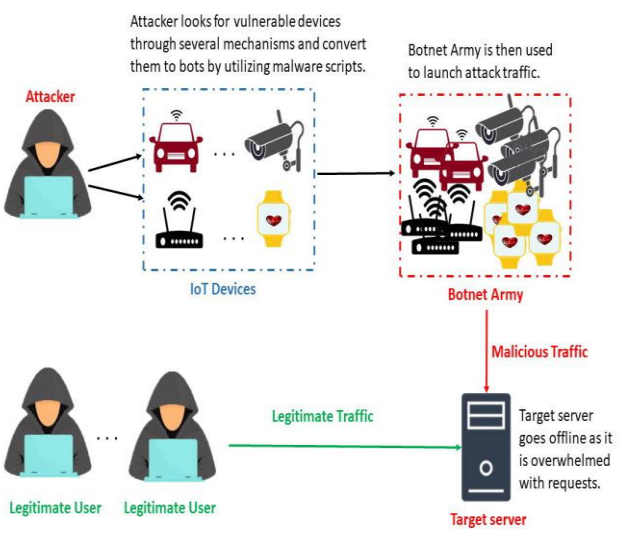

Figure 5 An illustration showing an attacker gaining access to IoT devices and initiating DDoS attacks[3].

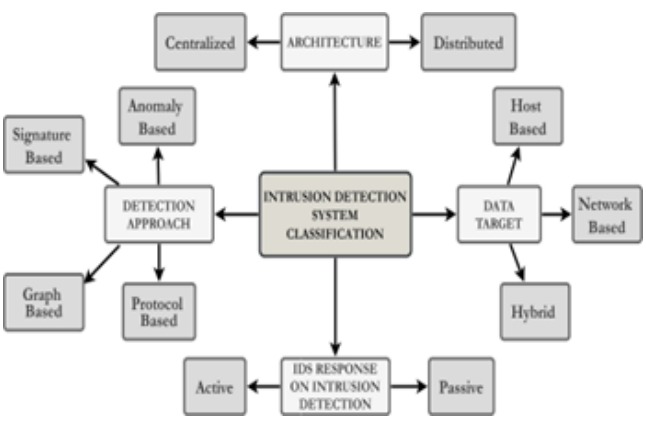

Figure 6 A visual depiction of the classification of different IDS techniques[3].

IV. CONCLUSION

The rapid growth of IoT has revolutionized various sectors but also introduced security challenges. Key concerns include vulnerabilities across IoT layers, cybersecurity principles (confidentiality, integrity, availability), and the threat of DDoS attacks. IoT devices in critical fields like healthcare and defense are particularly at risk from cyber threats such as botnet-based attacks.To address these issues, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play crucial roles. IDS monitors and detects malicious activities, while IPS actively blocks threats. The study stresses the need for improved security frameworks, focusing on detecting and mitigating IoT threats. Future work aims to develop a generalized IDS model for better protection and a more secure IoT ecosystem.

REFERENCE

[1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, ``A survey of machine and deep learning methods for Internet of Things (IoT) security," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 16461685, 3rd Quart., 2020.

[2] R. Hassan, F. Qamar, M. K. Hasan, A. Hazah, M. Aman, and A. S. Ahmed, ``Internet of Things and its applications: A comprehensive survey," Symmetry, vol. 12, no. 10, p. 1674, 2020.

[3] S. P. Dash, ``The impact of IoT in healthcare: Global review," J. Indian Inst. Sci., vol. 100, no. 4, pp. 773785, 2020.

[4] K. Demestichas, N. Peppes, and T. Alexakis, ``Survey on security threats in agricultural IoT and smart farming," Sensors, vol. 20, no. 22, p. 6458, Nov. 2020.

[5] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, ``Evolution of IoT-enabled connectivity and applications in automotive industry: A review," Veh. Commun., vol. 27, pp. 115, Jan. 2021.

[6] N. K. Suryadevara and G. R. Biswal, ``Smart plugs: Paradigms and applications in the smart city-and-smart grid," Energies, vol. 12, no. 10, pp. 120, 2019.

[7] S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, ``Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions," Comput. Sci. Rev., vol. 38, Nov. 2020, Art. no. 100303.

[8] S. C. Eimler, N. C. Krämer, and A. M. Von Der Pütten, ``Empirical results on determinants of acceptance and emotion attribution in confrontation with a robot rabbit," Appl. Artif. Intell., vol. 25, no. 6, pp. 503529, 2011.

[9] [9] M. Miraz, M. Ali, P. Excell, and R. Picking, ``Internet of nano-things, things and everything: Future growth trends," Future Internet, vol. 10, no. 8, p. 68, Jul. 2018.

[10] [10] Q.-D. Ngo, H.-T. Nguyen, L.-C. Nguyen, and D.-H. Nguyen, ``A survey of IoT malware and detection methods based on static features," Opt. Commun., 2020, Art. no. 126175.

[11] [11] I. Zafeiriou, ``IoT and mobility in smart cities," in Proc. 3rd World Symp. Commun. Eng. (WSCE), 2020, pp. 9195.

[12] [12] T. S. Bharati, ``Internet of Things (IoT): A critical review," Int. J. Sci. Technol. Res., vol. 8, no. 10, pp. 227232, 2019.

[13] [13]A. Pal, H. K. Rath, S. Shailendra, and A. Bhattacharyya, ``IoT standardization: The road ahead," in Proc. IntechOpen, 2018, pp. 5374.

[14] [14] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, ``Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," Int. J. Commun. Syst., vol. 33, no. 12, pp. 140, 2020.

[15] [15] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, ``IoT connectivity technologies and applications: A survey," IEEE Access, vol. 8, pp. 6764667673, 2020.

[16] [16]Hussain, I. (2024). Secure, sustainable smart cities and the internet of things: Perspectives, challenges, and future directions. *Sustainability*, *16*(4), 1390.

[17] [17]Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. *Future Internet*, *16*(2), 40.

[18] Baniya, P., Agrawal, A., Abid, K., Nath, J., Chaudhary, B. K., & Kunwar, B. (2024, February). The Internet of Things: Security Challenges and Opportunities. In *2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)* (pp. 153-158). IEEE.

[19] Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare Internet of Things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal*, *11*(11), 19046-19069.

[20] Tawffaq, M. R., Jasim, M. A., Mejbel, B. G., Issa, S. S., Alamro, L., Shulha, V., & Aram, E. (2024, October). IoT Security in a Connected World: Analyzing Threats, Vulnerabilities, and Mitigation Strategies. In *2024 36th Conference of Open Innovations Association (FRUCT)* (pp. 626-638). IEEE.

[21] M. Burhan and R. A. Rehman, ``IoT elements, layered architectures and security issues: A comprehensive survey," Sensors, vol. 18, no. 9, pp. 137, 2018.

[22] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, ``Perception layer security in the Internet of Things," Futur. Gener. Comput. Syst., vol. 100, pp. 144164, Jan. 2019.

[23] O. S. J. Nisha and S. M. S. Bhanu, ``A survey on code injection attacks in mobile cloud computing environment," in Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Conuence), Jan. 2018, pp. 16.

[24] M. Devi and A. Majumder, ``Side-channel attack in Internet of Things: A survey," in Applications of Internet of Things (Lecture Notes in Networks and Systems), J. K. Mandal, S. Mukhopadhyay, and A. Roy, Eds Singapore: Springer, 2021, pp. 213222.

[25] K. O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, ``A survey on the security of low power wide area networks: Threats, challenges, and potential solutions," Sensors, vol. 20, no. 20, pp. 119, 2020.

[26] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ``A survey of IoT security based on a layered architecture of sensing and data analysis," Sensors, vol. 20, no. 13, pp. 120, 2020.

[27] K. Nirmal, B. Janet, and R. Kumar, ``Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection," Peer-Peer Netw. Appl., pp. 113, Jun. 2020.

[28] R. Vishwakarma and A. K. Jain, ``A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommun. Syst., vol. 73, no. 1, pp. 325, Jan. 2020.

[29] A. Raoof, A. Matrawy, and C.-H. Lung, ``Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks," IEEE Internet Things J., vol. 7, no. 12, pp. 1153611546, Dec. 2020.

[30] D. Dinculean and X. Cheng, ``Vulnerabilities and limitations of MQTT protocol used between IoT devices," Appl. Sci., vol. 9, no. 5, p. 848, Feb. 2019.

[31] A. Tewari and B. B. Gupta, ``Security, privacy and trust of different layersin Internet-of-Things (IoTs) framework," Future Gener. Comput. Syst., vol. 108, pp. 909920, Jul. 2020.

[32] B. Ahlawat, A. Sangwan, and V. Sindhu, ``IoT system model, challenges and threats," Int. J. Sci. Technol. Res., vol. 9, no. 3, pp. 67716776, 2020.

[33] B. Prabadevi and N. Jeyanthi, ``A review on various snifng attacks and its mitigation techniques," Indonesian J. Elect. Eng. Comput. Sci., vol. 12, no. 3, pp. 11171125, 2018.

[34] C. V. Martínez and B. Vogel-Heuser, ``Towards industrial intrusion prevention systems: A concept and implementation for reactive protection," Appl. Sci., vol. 8, no. 12, pp. 129, 2018.

[35] T. R. Glass-Vanderlan, M. D. Iannacone, M. S. Vincent, Q. Chen, and R. A. Bridges, ``A survey of intrusion detection systems leveraging host data," ACM Comput. Surv., vol. 52, no. 6, p. 128, 2018.

[36] R. Panigrahi, S. Borah, A. K. Bhoi, and P. K. Mallick, ``Intrusion detection systems (IDS)An overview with a generalized framework," Adv. Intell. Syst. Comput., vol. 1040, pp. 107117, Jan. 2020.

[37] A. N. Cahyo, A. K. Sari, and M. Riasetiawan, ``Comparison of hybrid intrusion detection system," in Proc. 12th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE), Oct. 2020, pp. 9297.