

Intrusion detection and prevention using Bayesian decision with fuzzy logic system

Satheeshkumar Sekar¹, Palaniraj Rajidurai Parvathy¹, Gopal Kumar Gupta²,
Thiruvengadachari Rajagopalan³, Chethan Chandra Subhash Chandra Basappa Basavaraddi⁴,
Kuppan Padmanaban⁵, Subbiah Murugan⁶

¹Mphasis Corporation, Chandler, United States of America

²Symbiosis Institute of Technology Nagpur Campus, Symbiosis International (Deemed University), Pune, India

³Department of Mathematics, University College of Engineering, Anna University, Ariyalur, India

⁴Department of Artificial Intelligence and Machine Learning, Don Bosco Institute of Technology, Bangalore, India

⁵Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

⁶Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India

Article Info

Article history:

Received Mar 20, 2024

Revised Sep 6, 2024

Accepted Oct 1, 2024

Keywords:

Bayesian decision algorithm

Denial of service

Fuzzy logic system

Intrusion detection and prevention

Queue management

ABSTRACT

Nowadays, intrusion detection and prevention method has comprehended the notice to decrease the effect of intruders. Denial of service (DoS) is an attack that formulates malicious traffic is distributed into an exacting network device. These attackers absorb with a valid network device, the valid device will be compromised to insert malicious traffic. To solve these problems, the Bayesian decision model with a fuzzy logic system based on intrusion detection and prevention (BDFL) is introduced. This mechanism separates the DoS packets based on the type of validation, such as packet and flow validation. The BDFL mechanism uses a fuzzy logic system (FLS) for validating the data packets. Also, the key features of the algorithm are excerpted from data packets and categorized into normal, doubtful, and malicious. Furthermore, the Bayesian decision (BD) decide two queues as malicious and normal. The BDFL mechanism is experimental in a network simulator environment, and the operations are measures regarding DoS attacker detection ratio, delay, traffic load, and throughput.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Gopal Kumar Gupta

Symbiosis Institute of Technology Nagpur Campus, Symbiosis International (Deemed University)

Lavale, Mulshi, Pune, Maharashtra 412115, India

Email: gopalgupta.iitbhu90@gmail.com

1. INTRODUCTION

The modern creation of intrusion detection systems (IDS) growingly demands machine-controlled and intelligent IDS to deal with threats, causing a rise in the number of encouraged attackers in the cyber environment [1]. Specifically, there have been great necessitates for autonomous agent-based IDS solutions that necessitate as little human interference as feasible when being capable of developing and enhancing itself and developing into more robust to probable threats. Enhancing cybersecurity by detecting and preventing intrusions at endpoints using machine learning algorithms is a successful strategy [2]. Traditional intrusion detection and prevention methods often depend on signature-based approaches. However, these methods may not be enough to identify fresh and complex assaults. On the other hand, algorithms that learn via machine learning can evaluate patterns, behaviors, and anomalies within the data to detect possible risks in real-time [3].

Denial of service (DoS) and distributed denial of service (DDoS) are both well-known types of assaults that have the same goal, which is to exhaust the computing capabilities of a host or target. Network, making them inaccessible to legitimate users who are allowed to use them or adversely harming the performance of their computer system in some way [4]. DoS attacks may be broken down into a few different kinds, the most common of which are software vulnerabilities and flooding attacks [5]. When an attacker utilizes software exploits, they are taking advantage of vulnerabilities in their target server to either completely cease the services being provided by the server or drastically degrade the performance it is capable of. In the event of flooding attacks, the attacker uses up all of the system's resources by sending many incorrect requests, leading to the challenges discussed in the previous section. The most recent version of the DDoS takes advantage of multiple network components' power to increase the threat caused by the attack by distributing it across slave machines [6]. Implementing machine learning (ML) based intrusion detection and prevention at endpoints requires carefully choosing appropriate algorithms, quality data, and ongoing monitoring and adaptation. By continuously refining the models and integrating them into the security workflow, organizations can significantly enhance their ability to detect and prevent intrusions at the endpoint level [7].

Research gap: an intelligent IDS is introduced for the security internet protocol (IP) multimedia subsystem (IMS) by applying ML to raise classifier accuracy, this mechanism chooses vital features to build an IDS. This mechanism presents the decision tree (DT), support vector machine (SVM), as well as Naive Bayesian classifier to measure intrusion detection efficiently. However, these classifiers cannot detect the DoS attack efficiently [8]. To solve these issues intrusion detection and prevention using Bayesian decision with fuzzy logic system is proposed. The remainder of the paper is structured as follows. Section 2 discusses the Bayesian decision model with a fuzzy logic system based on intrusion detection and prevention. The network simulation analysis is specified in section 3. Finally, we conclude the paper in section 4.

Intrusion prevention system (IPS) detects cyber-attacks by applying machine learning algorithms like SVM and forest algorithm [9]. Hacking identification through the fuzzy logic system using the fuzzy algorithms to notice the injection attacks [10]. However, it creates important errors. Graph-based intrusion detection system introduces the sequence of interchanged messages. Though, it cannot notice attacks by analyzing separated frames and also has an important error [11]. IDS is highly proficient, but it is also able to detect threats. The anomaly detection system is capable of discovering anomalies with a lesser false positive and false negative. This mechanism recognizes deep learning to enhance scalability and efficiency. Feature standardization can utilize to raise accuracy. Different feature selection mechanisms to choose certain features that can manipulate results better. However, this mechanism raises the network traffic [12].

A deep Q-learning method offers an auto-learning capability for an environment that can distinguish several network intrusions. This mechanism caught and examined to notice malicious payloads in a self-learning fashion. However, this mechanism does not use the cloud environment [13]. A neural network with deep learning (DL) is the most appropriate for detecting DoS attacks that have reached high-performance accuracy. However, this mechanism does not guarantee they optimally categorize unidentified packets incoming through a web server because the identification possibility is high but has a degree of insecurity [14]. The intrusion detection and prevention system apply model-based intrusion detection and ML-based intrusion prevention to defend the network. The detection phase reduces network features and examines them to determine whether the network is in a normal state. This mechanism utilizes Q-learning and, throughout interactions, discovers the best scheme against an attack [15].

Cyber defense demands functions conducted in the cybersecurity field, defending mission targets to recognize and avoid cyberattacks, including IDS, as well as intrusion prevention. Explainable Artificial Intelligence algorithm for anomaly-based IDS in internet of things (IoT) networks. Initially, the IDSs concentrate on anomaly-based detection techniques to offer trust and confidence. Next, utilize DL to efficiently detect an anomaly, providing better performances [16]. ML algorithms act a vital task in building an IDS. An ensemble method using random subspace in that an extreme learning machine is preferred as the base classifier. An ensemble pruning method was established on the bat algorithm fitness function to enhance the classifier subset [17]. A deep reinforcement learning algorithm that utilizes the Markov decision process to enhance the IDS decision operation. This mechanism provides better detection performance and minimizes the false alarm count. However, this mechanism does not detect the doubtful attacker [18]. A federated deep reinforcement learning-based IDS in that several agents are distributed on the network, and these agents extend a deep Q-network logic. It conceived every agent's data privacy occupied while designing the system, and every agent does not distribute the data to other nodes [19].

Multi-agent feature selection-based IDS constitutes a feature self-selection and a deep reinforcement learning attack detection. The feature self-selection method purchases multi-agent reinforcement learning that specifies the issues of feature selection. Furthermore, it minimizes the complexity and improves the search strategy to choose the feature. Moreover, the graph convolutional network method evokes deeper features from the data. This mechanism enhances the accuracy [20]. The threat of DDoS has developed with the

increase of intelligent information systems. This mechanism utilizes a decision tree-based model to detect DDoS attacks [21]. Cyber security approaches to enhance the security evaluates against cyber-attacks. Conventional security solutions describing and developing security threats [22]. The wireless fidelity (Wi-Fi)-enabled energy observing for solar-powered buildings that will permit for daily and weekly learn of energy utilize [23]. IDS purpose is to extend the security in an IoT environment [24]. Distributed multi-agent IDS utilized learning agents separate the normal or attack based on network behavior [25]. The Bayesian decision (BD) model established a reliable route formation and it separates an unreliable sensor and forward the data efficiently [26]. The IDS using an ensemble model to design a smart homes to recognize the attacks [27].

2. PROPOSED METHOD

The intrusion prevention system (IPS) is an extensive IDS that assists in observing all normal models of traffic and transmits alerts in case of any difference from the normal model. Since the public can granted access to the network, the data packets forward from intruders are combined into the network traffic as input. It is essential to observe all inward and departing traffic. The data packets from the valid users come into switches, whereas the data packets are corroborated utilizing features. Although the attackers are intercepted, the compromised user's involvement is present in the network. The compromised users distribute malicious packets to all nodes, draining the network resources. This mechanism detects and prevents intrusion like DoS attacks based on packet and flow classifiers. Figure 1 explains the structure of the Bayesian decision model with a fuzzy logic system (BDFL) approach.

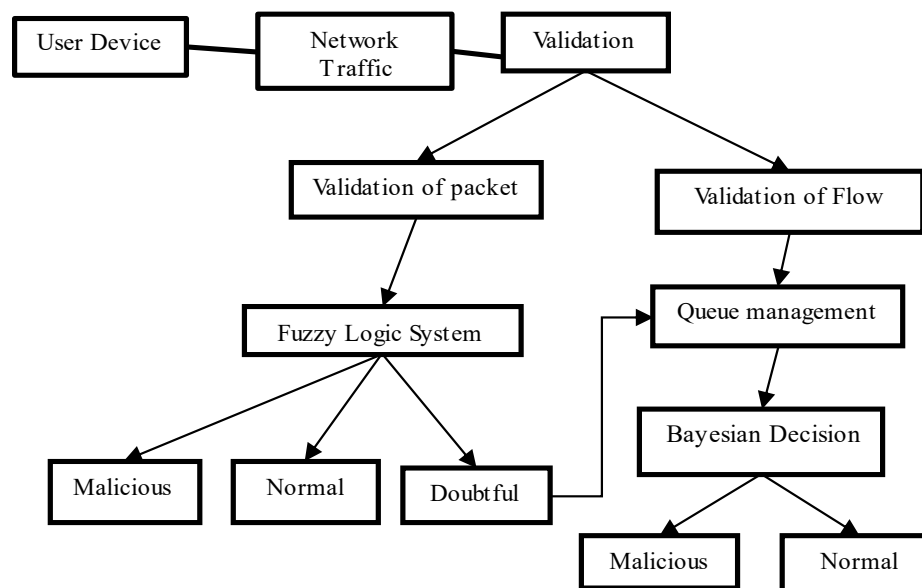


Figure 1. Structure of BDFL approach

From Figure 1, the upcoming data packet is validated by fuzzy logic system (FLS) membership functions and the queue management validates the data flow. The inwards packets are classified malicious, normal and doubtful; thus, separates an abnormal behavior. Then, the Bayesian decision algorithm checks the doubtful packet queue. If checked the packet is an abnormal behavior type, it is distinguished as the attack and invokes the alarm as a signal to the appreciated device holder. Thus, the BDFL mechanism utilizing Intelligent IDS for determining whether the performance of traffic is normal or not.

2.1. FLS-based DoS attack detection

The packet-based validation module that detects the DoS by the FLS. Here, the input packet features are excerpted from the packet header, like sender and receiver address, type of protocol, and sender and receiver port [28]. The obtained inputs are confirmed with the principles, and it makes an output like normal, doubtful, and malicious packets. The rightness of the packet feature defines the FLS. Figure 2 explains FLS-based DoS attack detection and Table 1 shows FLS table.

Table 1. FLS table

Type of Protocol	Sender and receiver address	Sender and receiver port	Output
High(H)	High	Low (L)	Normal packet
Middle (M)	Middle	Middle	Doubtful packet
High	Low	High	Malicious packet

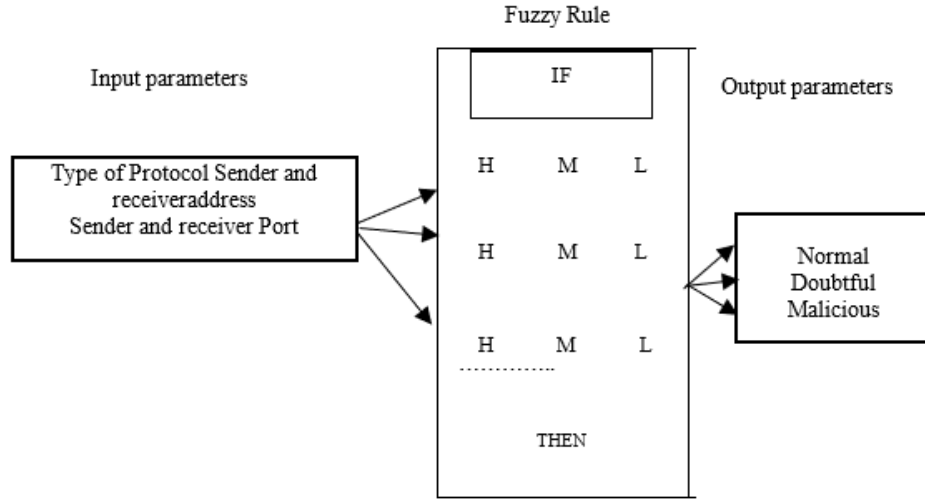


Figure 2. FLS-based DoS attack detection

Inwards packets from normal users are purified, and therefore, the usage of overload bandwidth is minimized. Bandwidth is a necessary resource to operate the arrived packets. Thus, the bandwidth deficiency creates heavy packet loss. The inward packets correspond with the fields; the features are expressed for purified action. The purification is an important function of key packets from individual users. The function of filtration is to evade distributing malicious traffic at a preliminary stage. The FLS output displays normal, Doubtful, and malicious packets. Then, the normal packets are transferred, the malicious packets are rejected, and the packet bandwidth verifies the packet.

2.2. Queue management system-based DoS attack detection

In this mechanism, the doubtful packet is verified by the BD algorithm. The packet overflow is also encountered in the queue because of the intrusion involvement. Before confirming the flow, the bandwidth expenditure is evaluated. Because the bandwidth is the fundamental resource extremely engaged by intrusions and is not appropriated for normal packets, it presents two queues, such as: normal queue (NQ) malicious queue (MQ).

The data packets that are partly coupled with the fuzzy rule activity are treated. Alternatively, the packets in doubtful are explicit within the port as well as out port number. All inwards doubtful packets are treated one at a time using BD algorithm. The specified traces are applied in developing a rational decision from true evidence. Here, the BD algorithm is applied to decide the possibilities of specific event types. The trace is employed to calculate the conditional probability for variables with specified information regarding packet queue. The BD algorithm in Bayes' rule is utilized to inform the possibility of evaluating a trace as an additional confirmation. The BD algorithm applies to the NQ, and the MQ is specified in (1) and (2). Here, n_i denotes the total queue, MQ represents the malicious queue, and NQ explains a normal queue.

$$P(MQ|n_i) = \frac{P(MQ)*P(n_i|MQ)}{P(n_i)} \tag{1}$$

$$P(NQ|n_i) = \frac{P(NQ)*P(n_i|NQ)}{P(n_i)} \tag{2}$$

The queue possibility is greater than the threshold when the user queue is identified in action detection; the BD determines whether normal or malicious queue. The value of the threshold is present among 0 to 1. The threshold value is set to 0.5, and the possibility is better than a threshold that queue is normal or malicious in the network.

3. SIMULATION ANALYSIS

This mechanism utilizes a network simulator-3 to evaluate the network performance [29]. It builds a flow table in the entity OpenFlow switch based on that inwards packet is either lost or transmitted. This mechanism applies the simulation parameters to plan the proposed system. The objective of this mechanism is to distinguish and alleviate the DoS attackers in the network; thus, the parameters preferable in this mechanism are delay, detection ratio, throughput, and traffic load in the network [30]. The detection rate is a vital parameter that represents the efficient forecasting of DoS attacks. Figure 3 explains a detection ratio of SVM [31], DT, and BDFL approaches based on DoS attacker.

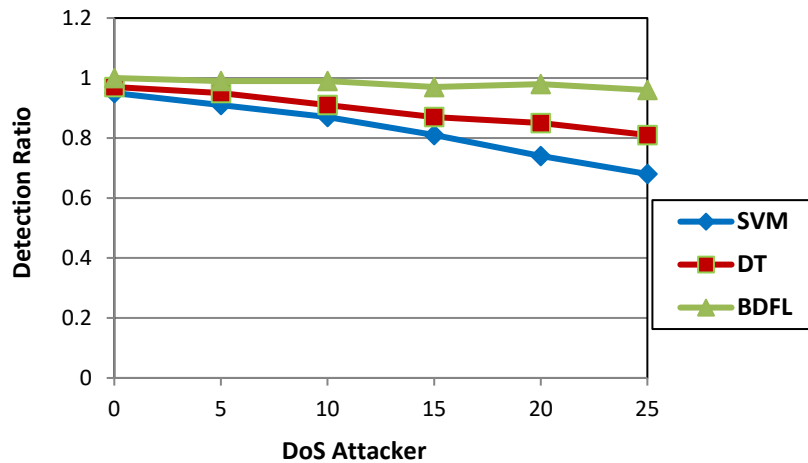


Figure 3. Detection ratio of SVM, DT, and BDFL approaches based on DoS attacker

From this result, the BDFL mechanism has a greater detection ratio at raising an attacker count. This raise is because of the suitable recognition of attacks utilizing FLS and BD algorithms. The preliminary level *i.e.*, without DoS attacker for BDFL, SVM and DT mechanisms detection ratio is 1, 0.97, and 0.95. The existing SVM and DT-based IDS mechanisms that the packets are recognized as normal or malicious; however, it raises the false alarm. The proposed BDFL mechanism detects the compromised packets efficiently, however, the SVM and DT-based IDS mechanisms cannot detect the compromised packets efficiently.

Traffic load is a significant parameter in intrusion detection and prevention where the contribution of the DoS attackers is noticed. Most regularly, the DoS attacker's objective is to exhaust all the resources. The enlargement in irregular traffic load decides which attack packets may be involved. The traffic load for DT, SVM, and BDFL is displayed in Figure 4, respecting the rise in number of DoS attackers.

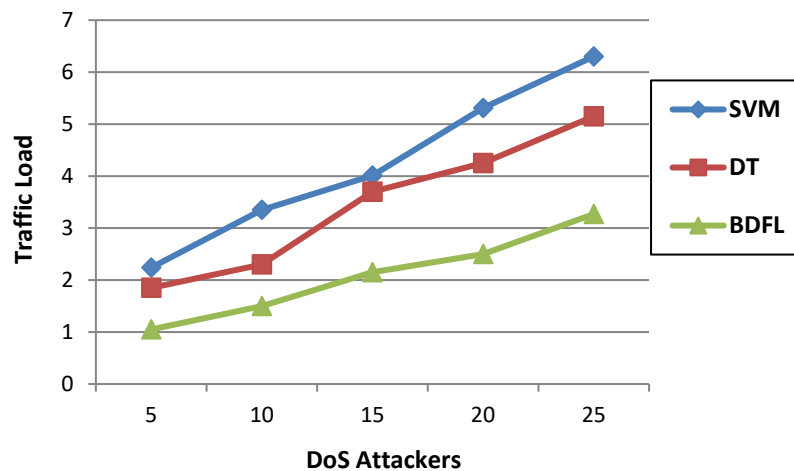


Figure 4. Traffic load of SVM, DT, and BDFL approaches based on DoS attacker

The rise in traffic load depletes a higher amount of bandwidth. This is minimized by appropriating normal users for requesting their service. In accordance with the DoS malicious packets, the BDFL mechanism is correctly recognized based on categorizing queue; as a result, it minimizes the traffic load. However, the DT and SVM algorithm does not accurately detect the malicious node; thus, it creates more traffic load.

Delay is a vital parameter, and the smaller delay will surely enhance the network performance. Generally, a rise in attack packets will ultimately enhance delay and minimize the throughput. The BDFL mechanism detects the DoS attack based on the FLS system and queue method. The development of malicious packets utilizes greater resources, and it causes disgrace to the performances of normal packets. Figure 5 compares delay parameters for SVM, DT, and BDFL mechanisms.

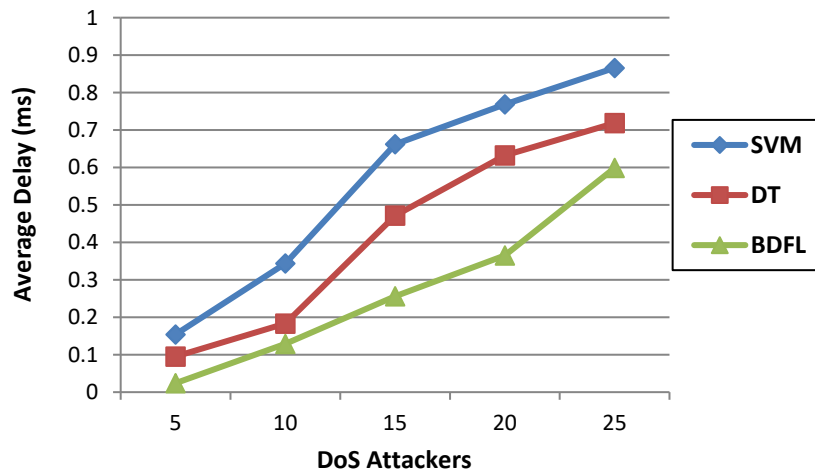


Figure 5. Delay of SVM, DT, and BDFL approaches based on DoS attacker

The alleviation of dishonest users with the action of malicious packets modifies to enhance delay. The delay increases with the rise in DoS attackers because of the participation of several DoS attackers who can handle the packets. IDS utilizing SVM and DT algorithms detect the DoS attackers but cannot detect the malicious packets efficiently. The proposed method uses the FLS and BD to detect malicious packets efficiently, hence reducing the network delay.

The network throughput rises while accessibility of bandwidth resource is adequate for the packet to procedure. In the network, the bandwidth utilization is a main restraint that will be engaged while the attack packets raise. Figure 6 explains the network throughput of SVM, DT, and BDFL mechanisms based on DoS attackers.

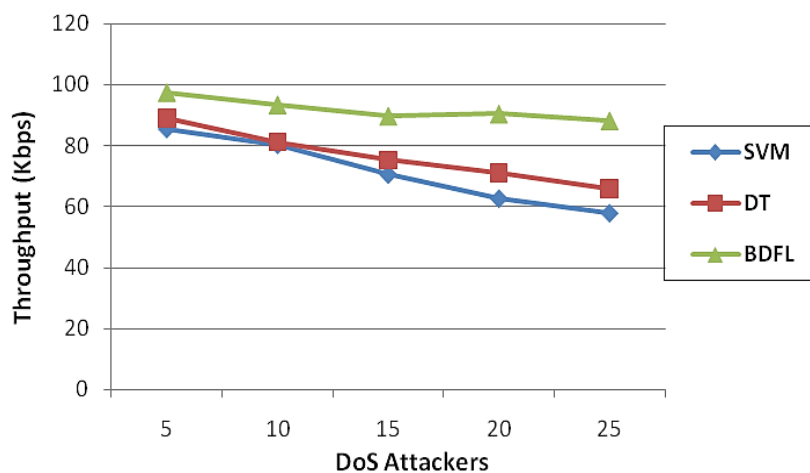


Figure 6. Throughput of SVM, DT, and BDFL approaches based on DoS attacker

In the proposed BDFL mechanism, the rapid rejection of malicious packets raises the bandwidth availability by applying the BD algorithm. The FLS algorithm also separates the malicious packets efficiently. Thus, the throughput is raised when compared with DT and SVM algorithms. But, the existing DT and SVM algorithms cannot detect the malicious data packet, and data flow well since the participation of DoS attacker is the main reason for raising attack packets.

4. CONCLUSION

In this section, a Bayesian decision model with a fuzzy logic system based on intrusion detection and prevention mechanism is planned particularly to guarantee security. This mechanism detects and prevents intrusion like DoS attacks based on packet and flow classifiers. The inwards packets are authenticated by applying FLS that provides the output of the packet as normal, malicious, and doubtful packets. Then, the doubtful packets are validated based on queue bandwidth. This mechanism applied the BD algorithm to separate the normal and malicious packets in the network. The simulation results illustrate the BDFL mechanism enhances the detection ratio and minimizes the network delay. Furthermore, the BDFL approach reduces the traffic load since the queue management process did only doubtful packets; thus, it reduces the network traffic load. In the future, we will utilize an ensemble learning algorithm to improve the IPS in a large-scale setting.





REFERENCES

- [1] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
- [2] M. F. Kabir and S. Hartmann, "Cyber security challenges: an efficient intrusion detection system design," in *2018 International Young Engineers Forum (YEF-ECE)*, May 2018, pp. 19–24. doi: 10.1109/YEF-ECE.2018.8368933.
- [3] A. Aldaej, "Enhancing cyber security in modern internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI)," *IEEE Access*, p. 1, 2021, doi: 10.1109/ACCESS.2019.2893445.
- [4] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, pp. 1–12, Dec. 2017, doi: 10.1177/1550147717741463.
- [5] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *Journal of Network and Computer Applications*, vol. 136, pp. 71–85, Jun. 2019, doi: 10.1016/j.jnca.2019.03.005.
- [6] T. E. de Sousa Araújo, F. M. Matos, and J. A. Moreira, "Intrusion detection systems' performance for distributed denial-of-service attack," in *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Oct. 2017, pp. 1–6. doi: 10.1109/CHILECON.2017.8229519.
- [7] S. Singh, R. Sulthana, T. Shewale, V. Chamola, A. Benslimane, and B. Sikdar, "Machine-learning-assisted security and privacy provisioning for edge computing: a survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 236–260, Jan. 2022, doi: 10.1109/JIOT.2021.3098051.
- [8] C.-Y. Hsu, S. Wang, and Y. Qiao, "Intrusion detection by machine learning for multimedia platform," *Multimedia Tools and Applications*, vol. 80, no. 19, pp. 29643–29656, Aug. 2021, doi: 10.1007/s11042-021-11100-x.
- [9] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for CAN: hindering cyber-attacks with a low-cost platform," *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.
- [10] F. Martinelli, F. Mercaldo, V. Nardone, and A. Santone, "Car hacking identification through fuzzy logic algorithms," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Jul. 2017, pp. 1–7. doi: 10.1109/FUZZ-IEEE.2017.8015464.
- [11] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 1727–1736, Mar. 2022, doi: 10.1109/TITS.2020.3025685.
- [12] A. Vikram and Mohana, "Anomaly detection in network traffic using unsupervised machine learning approach," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Jun. 2020, pp. 476–479. doi: 10.1109/ICCES48766.2020.9137987.
- [13] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," *Computers*, vol. 11, no. 3, pp. 1–19, Mar. 2022, doi: 10.3390/computers11030041.
- [14] J. F. Canola Garcia and G. E. T. Blandon, "A deep learning-based intrusion detection and prevention system for detecting and preventing denial-of-service attacks," *IEEE Access*, vol. 10, pp. 83043–83060, 2022, doi: 10.1109/ACCESS.2022.3196642.
- [15] P. Jokar and V. C. M. Leung, "Intrusion detection and prevention for ZigBee-based home area networks in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1800–1811, 2018, doi: 10.1109/TSG.2016.2600585.
- [16] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the Internet of Things: opportunities and solutions," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023, doi: 10.1109/COMST.2023.3280465.
- [17] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu, and Y. Yang, "An ensemble method based on selection using bat algorithm for intrusion detection," *The Computer Journal*, vol. 61, no. 4, pp. 526–538, Apr. 2018, doi: 10.1093/comjnl/bxx101.
- [18] H. Benaddi, K. Ibrahim, A. Benslimane, and J. Qadir, "A deep reinforcement learning based intrusion detection system (DRL-IDS) for securing wireless sensor networks and Internet of Things," in *12th EAI International Conference, WiCON 2019, TaiChung, Taiwan, November, 2020*, pp. 73–87. doi: 10.1007/978-3-030-52988-8_7.
- [19] S. Vadigi, K. Sethi, D. Mohanty, S. P. Das, and P. Bera, "Federated reinforcement learning based intrusion detection system using dynamic attention mechanism," *Journal of Information Security and Applications*, vol. 78, pp. 1–12, Nov. 2023, doi: 10.1016/j.jisa.2023.103608.





- [20] K. Ren, Y. Zeng, Y. Zhong, B. Sheng, and Y. Zhang, "MAFSIDS: a reinforcement learning-based intrusion detection model for multi-agent feature selection networks," *Journal of Big Data*, vol. 10, no. 1, pp. 1–30, Sep. 2023, doi: 10.1186/s40537-023-00814-4.
- [21] W. Alhalabi, A. Gaurav, V. Arya, I. F. Zamzami, and R. A. Aboalela, "Machine learning-based distributed denial of services (DDoS) attack detection in intelligent information systems," *International Journal on Semantic Web and Information Systems*, vol. 19, no. 1, pp. 1–17, Aug. 2023, doi: 10.4018/IJSWIS.327280.
- [22] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A. Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2023, pp. 1755–1759. doi: 10.1109/ICECA58529.2023.10394962.
- [23] R. Krishna Vanakamamidi, L. Ramalingam, N. Abirami, S. Priyanka, C. S. Kumar, and S. Murugan, "IoT security based on machine learning," in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Aug. 2023, pp. 683–687. doi: 10.1109/SmartTechCon57526.2023.10391727.
- [24] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion detection and prevention system for an IoT environment," *Digital Communications and Networks*, vol. 8, no. 4, pp. 540–551, Aug. 2022, doi: 10.1016/j.dcan.2022.05.027.
- [25] A. Javadpour, P. Pinto, F. Ja'fari, and W. Zhang, "DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments," *Cluster Computing*, vol. 26, no. 1, pp. 367–384, Feb. 2023, doi: 10.1007/s10586-022-03621-3.
- [26] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.
- [27] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.
- [28] D. Javaheri, S. Gorgin, J.-A. Lee, and M. Masdari, "Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: classification, overview, and future perspectives," *Information Sciences*, vol. 626, pp. 315–338, May 2023, doi: 10.1016/j.ins.2023.01.067.
- [29] S. K. Sekar *et al.*, "Random forest algorithm with hill climbing algorithm to improve intrusion detection at endpoint and network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 37, no. 1, p. 134, Jan. 2025, doi: 10.11591/ijeecs.v37.i1.pp134-142.
- [30] P. Radhakrishnan *et al.*, "DoS attack detection and hill climbing based optimal forwarder selection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 2, p. 882, Nov. 2024, doi: 10.11591/ijeecs.v36.i2.pp882-891.
- [31] A. Ponnmalar and V. Dhanakoti, "An intrusion detection approach using ensemble support vector machine based chaos game optimization algorithm in big data platform," *Applied Soft Computing*, vol. 116, p. 108295, Feb. 2022, doi: 10.1016/j.asoc.2021.108295.

BIOGRAPHIES OF AUTHORS






Satheeshkumar Sekar     with over 15 years of seasoned expertise in information technology, he brings a wealth of experience spanning project and portfolio management, technical delivery, and managed services. His extensive background includes a strong focus on data and cloud projects, where he has excelled in system analysis, requirement gathering, design, development, testing, quality assurance, implementation, and support across banking, insurance, healthcare, and manufacturing domains. Notable skills include proficiency in snowflake, Azure Databricks, and Azure services, with a special emphasis on HVR real-time replication. He has successfully managed end-to-end project planning, execution, and management, aligning activities with core business objectives. His competencies extend to data analysis, governance, integration, quality, application tuning, and security. He has demonstrated mastery in developing custom Python utilities for seamless data migration and exhibits hands-on experience in Spark, Scala, Python, and UNIX shell scripting. A standout achievement includes designing and building HVR ELT pipelines for various platforms, highlighting his expertise in data movement. Furthermore, his background encompasses reengineering legacy applications into microservices on the Databricks platform and executing successful Teradata to Snowflake migrations and Teradata to GCP BigQuery. Well-versed in Azure DevOps and Databricks MLOps, he brings a comprehensive understanding of tools and technologies in IBM mainframe, vision plus, and IDMS. He can be contacted at email: satheeshkumar.sekar24@gmail.com.






Palaniraj Rajidurai Parvathy     is a project manager at Mphasis Corporation in Chandler, Arizona, USA. He has over 16 years of IT experience in the BI and analytics domain, with a focus on data modeling, integration, and visualization (Snowflake, Azure, AWS, GCP, Azure Data Factory, Databricks, Tableau, Power BI, Python, R, SAP BO, Alteryx, Xceptor (RPA)). He has been recognized by customers for providing "customer value addition" through performance tuning on schedule. He received the "star performer" award of the quarter for a support project from Hexaware leadership. Additionally, he was awarded the "Star Performer" award of the quarter for a migration project from Hexaware leadership. Moreover, he was recognized as the "Most valuable player" for a support project from Wipro - best buy account leadership. He also received a "Feather in my cap" award for outstanding contribution to the project business group hierarchy iteration. He can be contacted at email: palanirajrps@gmail.com.






Gopal Kumar Gupta    did his Master's in mathematics from Banaras Hindu University, Varanasi, Uttar Pradesh, India, in 2011. He earned his Ph.D. degree in 2019 from the Department of Mathematical Sciences, Indian Institute of Technology, Banaras Hindu University, Varanasi, Uttar Pradesh, India. He is currently working as an assistant professor at the Symbiosis International University Nagpur campus, India. He has published research papers in various journals, such as the International Journal of Quality Technology and Quantitative Management, International Journal of Operational Research, International Journal of Applied and Computational Mathematics, and International Journal of Mathematics in Operational Research, among others. He can be contacted at email: gopalgupta.iitbhu90@gmail.com.






Thiruvengadachari Rajagopalan    is currently working with Anna University, University College of Engineering Ariyalur, Tamil Nadu, India. He has two decades of rich experience in teaching and research. His areas of research include linear algebra, applied algebra, and theoretical computer science. He was awarded a doctoral degree in 2012 by Bharathidasan University, Tiruchirapalli, Tamil Nadu, India. He is passionate and has been focused on conducting interdisciplinary research. He can be contacted at email: rajgopalant@gmail.com.






Chethan Chandra Subhash Chandra Basappa Basavaraddi    working as an associate professor in the Department of Artificial Intelligence and Machine Learning at Don Bosco Institute of Technology, Kumbalagodu, Bangalore-560074. He has over 12 years of rich experience in teaching at reputed institutions. He is also an accomplished researcher in the fields of artificial intelligence, deep learning, and image processing. To his credit, he has published many research articles in well-reputed journals and has filed patents as well. He can be contacted at email: raddi04@yahoo.com.



Kuppam Padmanaban    joined K L University in 2019 upon completing his Ph.D. in computer science and engineering. Currently, he serves as an associate professor in the Department of Computer Science and Engineering (Honors) at the School of Computing, Koneru Lakshmaiah Education Foundation, K L University, Andhra Pradesh, India. Specializing in full-stack development, he possesses expertise in various technologies, including MERN, Python, spring microservices, and the .NET framework. He holds bachelor's and master's degrees in computer science and engineering from Anna University in Tamil Nadu, India. His research focuses on wireless sensor networks, IoT, machine learning, and data analytics. He has published numerous research articles in reputable journals and conferences. He can be contacted at email: padmanaban.k@yahoo.com.



Subbiah Murugan    is an adjunct professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India. He published his research articles in many international and national conferences and journals. His research areas include network security and machine learning. He can be contacted at smuresjur@gmail.com.