

# Random forest algorithm with hill climbing algorithm to improve intrusion detection at endpoint and network

Satheesh Kumar Sekar<sup>1</sup>, Palaniraj Rajidurai Parvathy<sup>2</sup>, Latika Pinjarkar<sup>3</sup>, Raman Latha<sup>4</sup>,  
Mani Sathish<sup>5</sup>, Munnangi Koti Reddy<sup>6</sup>, Subbiah Murugan<sup>7</sup>

<sup>1</sup>Project Manager, Chandler, Arizona, USA

<sup>2</sup>Project Manager, Mphasis Corporation, Chandler, Arizona, USA

<sup>3</sup>Department of Computer Science and Engineering, Symbiosis Institute of Technology Nagpur Campus,  
Symbiosis international (Deemed) University, Pune, India

<sup>4</sup>Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Trichy, India

<sup>5</sup>Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India

<sup>6</sup>Department of Electronics and Communication Engineering, Universal College of Engineering and Technology, Guntur, India

<sup>7</sup>Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,  
Saveetha University, Thandalam, India

## Article Info

### Article history:

Received Feb 27, 2024

Revised Sep 6, 2024

Accepted Sep 29, 2024

### Keywords:

Endpoint security

Feature selection

Hill climbing algorithm

Intrusion detection

Random forest algorithm

## ABSTRACT

Cloud computing is a framework that enables end users to connect highly effective services and applications over the internet effortlessly. In the world of cloud computing, it is a critical problem to deliver services that are both safe and dependable. The best way to lessen the damage caused by entry into this environment is one of the primary security concerns. The fundamental advantage of a cooperative approach to intrusion detection system (IDS) is a superior vision of an action of network attack. This paper proposes a random forest (RF) algorithm with a hill-climbing algorithm (RFHC) to improve intrusion detection at the endpoint and network. Initially, it is used for feature selection, and the next process is to separate the intrusions detection. The feature selection is maintained by the hill climbing (HC) algorithm that chooses the best features. Then, we utilize the RF algorithm to separate the intrusion efficiently. The experimental results depict that the RFHC mechanism reached more acceptable results regarding recall, precision, and accuracy than a baseline mechanism. Moreover, it minimizes the miss detection ratio and enhances the intrusion detection ratio.

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



## Corresponding Author:

Latika Pinjarkar

Department of Computer Science and Engineering, Symbiosis Institute of Technology Nagpur Campus

Symbiosis international (Deemed) University

Pune, India

Email: latika.pinjarkar@sitnagpur.siu.edu.in

## 1. INTRODUCTION

The internet is applied to make possible entrée to the services provided by the cloud, acting as the main origin of threats that can taint the cloud resources and systems. Then, improving cloud security gets a main dispute for cloud providers [1]. Thus, many schemes, for example, data security, firewalls, authentication methods, and others, have been introduced to the best secure cloud surroundings from several attacks. Though, conventional systems are inadequate to secure cloud services from diverse limits [2]. In common parlance, an intrusion is defined as any unauthorized interference, and given that it is undesired or unauthorized, the motivation behind it is often malicious [3]. Once this information has been gathered, connections to the internal network will be initiated, and attacks will be carried out. In most cases, individuals from outside the company

are the ones that commit intrusions. In certain instances, intrusions may be triggered by internally authorized personnel who carry out these assaults by abusing their authority and moving outside their authorization area [4]. Platforms for endpoint detection and response assist security teams in locating suspicious behavior on endpoints, which enables them to eradicate threats more rapidly and reduce the damage caused by an attack. The term “endpoint detection and response” refers to a group of techniques that are used to identify and evaluate potential dangers posed by endpoints. The functions of detection, investigation, threat hunting, and reaction are often included in an EDR tool’s feature set [5]. An IDS is a useful adjunct to a firewall since it enables comprehensive inspections of data packets’ headers as well as their contents, offering protection against assaults that a firewall may otherwise misinterpret as apparently harmless network traffic [6]. Deep learning-based intrusion detection and prevention system (DLID) that detects the intrusion efficiently. This mechanism utilizes the deep learning algorithm to separate normal and malicious. The graphical user interface method shows diagrammatically and textually the data of captured and categorized packets. However, this mechanism provides less precision rate and increases the false positive rate and false alarm rate [7].

## 2. RELATED WORKS

The cloud computing system is increasing speedily, and it is appropriate for users to obtain services through the internet; it is suitable for arising, deploying, and getting mobile applications. Now, security is a necessary anxiety due to the open and disseminated nature of the cloud. Numerous amounts of data are accountable for appealing intrusion [8]. IDS is concentrated on boosting classification accuracy by enhancing the feature selection and considering the ensemble and the crow search algorithm (CSA). The choice of feature is handled by the filter method to receive the feature sets. The ensemble method creates the weights with the CSA to receive the best outcomes. However, this mechanism raises the utilization of calculation resources [9]. A cooperative to minimize the collision of denial of service (DoS) attacks in cloud computing. It assesses the dependability of this alert message through the majority vote method. Thus, IDSs organized in cloud computing regions exclude fatalities; one could avoid DoS attacks [10].

Detecting anomalies in the traffic on a network entails looking for patterns that are out of the ordinary and might point to potential vulnerabilities. The method can function by classifying network data via a collection of decision trees (DT), which in turn enables the detection of aberrant behaviors. The purpose of this mechanism is to better the accuracy and efficiency of identifying abnormalities within network traffic, with the ultimate goal of increasing overall network security [11]. Detection of anomalies-based intrusions in industrial data using support vector machine (SVM) and random forests (RF). The process of finding abnormal patterns or actions inside a system is what’s known as anomaly-based intrusion detection. SVM is used because of its capacity to classify data into several classes, differentiating normal activity from aberrant behavior in the process. On the other hand, RFs make use of a collection of DT to classify data, which increases precision [12]. RF algorithm is used to identify these irregularities and explain the identified abnormalities. The technique entails leveraging the RF model not just to find anomalies but also to give relevant explanations or insights into why these anomalies arose. The purpose of this study is to improve the interpretability of anomaly detection findings by understanding the decision-making process of the RF algorithm [13]. The explainable RF is to forecast unfavorable occurrences or activities known as anomalies accurately. The explainable RF offers clear and understandable insights into the study’s decision-making process. The purpose of adopting this model is to identify anomalies but also provide concise explanations. This strategy improves the interpretability of the findings of anomaly detection, allowing one to comprehend better the factors that led to the discovery of problems and to devise suitable solutions to avert unfavorable occurrences, leading to an increase in both productivity and security [14].

When carrying out local searching, an algorithmic optimization known as hill climbing (HC). To verify the current state, an HC search is the best option available in the area (the neighborhood) [15]. If it reaches the receiver in higher quality, it should be reexamined and stopped; otherwise, the current state should be revised in a more protracted condition. After that, repeat the stages until a result is reached or there are no signs of recent operator residue in the current state. If the latter is the case, the process is complete. In addition to this, the loop is now operating through two phases. To begin, the operator that has yet to be applied is chosen and then applied to the current state to create the fresh state. The last step is to verify if the condition is still fresh. From the phases that came before it, the best possible state quality will be presented in HC [16]. It acts as a guide to the quality of an invented solution. The advantages of healthcare management are controlling many concerns. The ability to tailor the approach and make changes to it is permitted according to this requirement. For instance, adaptability and the operation of distinct domains are carried out. The HC cause has been included in the newly developed strategy to enhance the capabilities of the local search. The HC method is the most straightforward approach to local searching. An arbitrary solution is used as a starting point, and the algorithm then shifts iteratively from a root-to-child solution until there are no best-child solutions left to identify. It does this by increasing the local searching capability, which is a required opinion of the HC approach.

Firewalls examine the control rules, and based on those rules, a packet is either permitted or refused. A host may be denied access to the trusted network based on a rule that defines whether or not they meet certain criteria. For a firewall to verify the rules, it just has to examine the header of the TCP/IP protocol, which may be FTP, HTTP, or Telnet [17]. On the other hand, it does not examine the information included in the network packet. As long as the header of the packet complies with the rules that have been set up in the firewall, it won't matter whether the data comprises harmful code or not; the firewall will still let the packet go through. Consequently, despite a firewall, an attack on your trusted network is still possible [18].

IDS is significant for detecting an anomaly in cloud computing that can be recognized as several attacks with fewer false positives. An effective IDS applying an ensemble-based learning method uses classifiers and a voting method. This detects the intrusion efficiently. However, it raises the required time for execution [19]. Feature Selection and intrusion forecasting to evaluate its effectiveness. The cooperative feature selection method incorporates time series analysis to recognize anomalies [20]. An efficient IDS applies an ensemble feature selection of precious minimized feature sets. The ensemble classifier is a vigorous classifier that forecasts the network traffic behavior [21]. Indian Sign Language (ISL) is the principal type of communication for most dumb and deaf citizens nationwide [22]. It is a developed natural language that has its lexicon as well as its syntax. Translation systems are essential to eliminate the communication barrier between the community of deaf and hard-of-hearing people. To facilitate effective two-way communication between the hearing-impaired and the general population of society, the proposed system is an end-to-end human interface architecture capable of recognizing and understanding spoken language and performing the necessary decoding of ISL signals. WSN is suitable for such applications due to their dense and dispersed sensing, tolerance to hostile conditions, and low power consumption. The research provides unique WSN deployment, data aggregation, and resource optimization methodologies for disaster management. These solutions will improve network coverage, dependability, and sensor longevity. The research also examines the synchronization of AI and human brainpower calculations with WSNs to enable smart navigation and robotized crisis response. The research study addresses WSN security and privacy in disaster management. It identifies flaws and suggests ways to classify, verify, and share data. A reenacted fiasco is used to evaluate the proposed alternatives. Situational awareness, response coordination, and emergency operations efficiency increase with the provided techniques [23]. Power quality monitoring offers forecasted insights into power quality fluctuations via examining past data and patterns that enhances grid stability as well as allocation of resources [24]. The system uses internet of things (IoT) sensors and cameras positioned in parking lots to track the occupancy status of specific parking spots in real-time. The acquired data is sent to a cloud server for analysis and processing. The convolutional neural network (CNN) algorithm, a deep learning approach, is used to evaluate the camera images and accurately determine if parking spots are occupied [25].

### 3. PROPOSED METHOD

The data pre-processing procedure is used to arrange them for selecting the feature. The training dataset contains binary, symbolic, and numerical data. This procedure takes clean as well as numeric inputs, so the dataset should be organized first. The Figure 1 steps operate the block diagram of the RFHC scheme and these components.

#### 3.1. Preprocessing

Taking out imperfect outliers unrelated, replica values and canceling features: in the dataset, we dropped features, for example, the IP address of the sender and receiver. In addition, the address of sender and receiver, timestamp and sender Port, and other features are removed. Feature mapping: represents the translating of the categorical variables into arithmetical form. One-hot encoding gives a superior classifier execution. The scaling of a feature is called data normalization, converting entire values from a set of features into a range of presets. Standardization is known as a Z-score normalization. Normalization (min-max) is the procedure of changing as well as resizing values, which drop in the series [0,1]. The min-max scaling equation is defined in (1).

$$X_k^* = \frac{(X_k - X_{min})}{(X_{max} - X_{min})} \quad (1)$$

Here,  $X_k$  is the preliminary value,  $X_k^*$  represents the data following development,  $X_{min}$  denotes the affecting data sequence's smallest value, and  $X_{max}$  indicates the highest value.

The information needed to collect in the class field is determined by the kind of assault. To facilitate identification, the class column has been partitioned into two distinct groups: normal and aberrant. Concerning the categorization of attacks, the class column is subdivided into the following categories: known and unknown attacks.

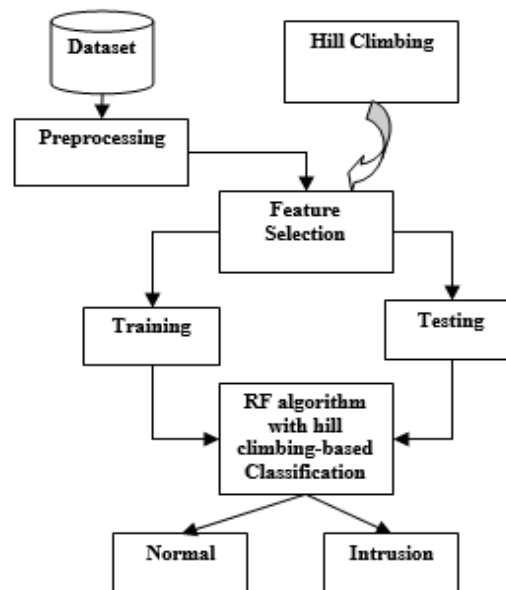


Figure 1. Block diagram of the RFHC scheme

### 3.2. Feature selection

It represents a pre-processing method that assists in selecting appropriate features. It reduces the dimensionality of data by minimizing unnecessary and unrelated attributes. While irrelevant features are appended to the classification procedure, reducing accuracy, it requires more space and time. Thus, the feature selection is vital because it is appropriate for a deeper realization of data by holding imperative suitable features, thus enhancing the classifier's accuracy, speed, and forecasting capacity. This mechanism utilizes an HC-based feature selection that shortlists important attributes.

The best-received result is next passed to the HC to speed up the search and defeat the slow convergence technique. HC is an iterative technique that initiates with a random resolution to a difficulty. Next, tries to decide on a better resolution by incrementally shifting a particular resolution component. When the adaptation builds the best solution, the additive update is fulfilled on the recent solution, which is repeated till no extra enhancements can be established.

### 3.3. Correlation of feature

It is a valuable method for feature engineering, as well as it is a numerical process that specifies the significance amongst one or more variables to notice the interrelated vital features. Next, the pre-processed data is split into two types, such as training as well as test dataset. In the training dataset, remove the features and create the different classifications in the test dataset.

### 3.4. RF-based intrusion detection

After the feature selection process, this mechanism uses an RF classifier algorithm trained with the two features picked out from a subset of the dataset to recognize intrusions. The RF algorithm concentrated on receiving reliable forecasting. The proposed method-based IDS contains selecting features to recognize and merge valuable features for precise identification. Once the feature subset is picked out, the RF classifier differentiates between an activity of real or intrusion. The RF classifier clusters several DT, and those outcomes are joined into one final output. This DT algorithm performs classification and regression. RF algorithm evades the over-adjustment issue.

Base classifiers use an  $m$  tree arrangement  $\{h(X, \delta_k), k=1,2..m\}$ . Here,  $X$  indicates the input data, and  $\delta$  depicts the dependent distributed random vector. Each DT picks out data arbitrarily from the usable data. Construct a forest to assemble the amount of trees  $k$  via reiterating the steps greater than for the amount of times  $k$ .

In training data, the RF algorithm provides less sensitivity to outlier data because of its ability to conquer the issue of overfitting. It is easy to launch parameters that evade the necessity for tree trimming. The RF algorithm admits an assembly of tree-structured learners, which every cast a major choice for the class with the most input. It is self-governing of prior random vectors of the same distribution, and an upper bound is derivative for RF to obtain the forecasting error.

#### 4. EXPERIMENTAL ANALYSIS

Experimental analyses are performed on the NSL-KDD datasets. We concentrate on classification models, and more specifically binary classification, since IDS, may become problematic while utilizing labeled data to try to determine whether or not an item is a member of the intrusion class [26]. The results returned by an algorithm for binary classification are either 0 or 1. Therefore, selecting the appropriate measure is essential for analyzing and verifying the RF algorithm. When dealing with issues of this kind, the metrics often include comparing the actual classes and the models' forecasts. This enables the estimated probability for these classes to be interpreted meaningfully. We are able to construct metrics such as accuracy, recall, and precision based on this mechanism, which will enable us to isolate infiltration using the RF method [27].

These metrics will help us to determine whether or not an event occurred. It consists of the following four variables: true positive (TP), true negative (TRN), false positive (FAP), and false negative (FAN). When evaluating the effectiveness of a model, each variable denotes a distinct meaning that is taken into account. For example, TRP suggests that the existence of dangers was accurately identified. On the other hand, TRN indicates that the lack of threats was accurately forecasted, which is a positive development. The fact that the model incorrectly predicted that there was no danger (FAN) and failed to identify the existence of the threat (FAP) suggests that the model did not adequately detect the presence of the threat. Accuracy (ACC) represents the percentage of precise predictions built in relation to all cases. ACC computation is specified in (2). Recall metric is applied to decide the percentage of suitably classified positive patterns. This calculation is specified in (3). Precision represents the expected patterns, and it counts the amount of precisely forecasted positive patterns in a positive class. This calculation is specified in (4). Figure 2 explains ANND and DDHC approaches for false positive ratio based on experiment count.

$$Acc = \frac{TRP+TRN}{TRP+FAN+FAP+TRN} \quad (2)$$

$$Rec = \frac{TP}{TP+FN} \quad (3)$$

$$Pr ec = \frac{TP}{TP+FP} \quad (4)$$

From Figure 2, the proposed RFHC mechanism uses the RF algorithm to detect the intrusion efficiently. Furthermore, it uses the hill climbing technique to select the features well. Conversely, the existing mechanism DLID increases the miss detection ratio since it is not performed during the network intrusion. Figure 3 explains DoS Intrusion detection ratio for RFHC and DLID mechanisms.

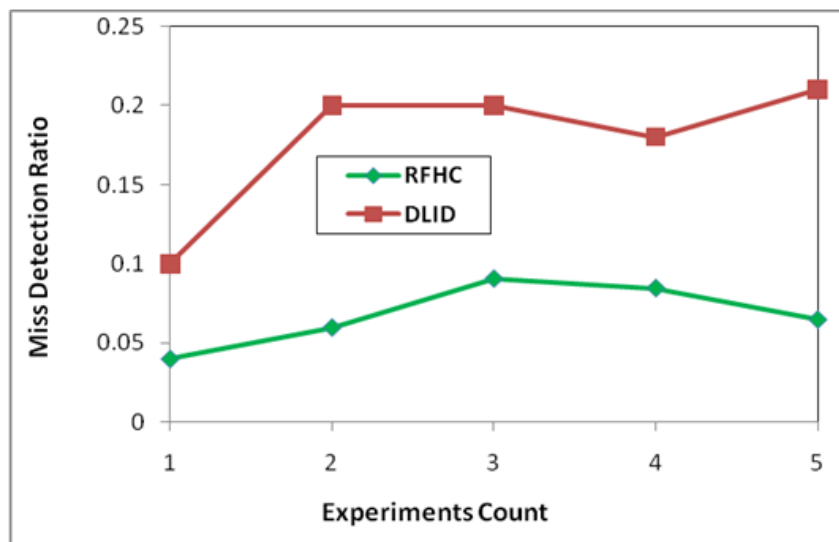


Figure 2. DLID and RFHC approach for miss intrusion detection ratio

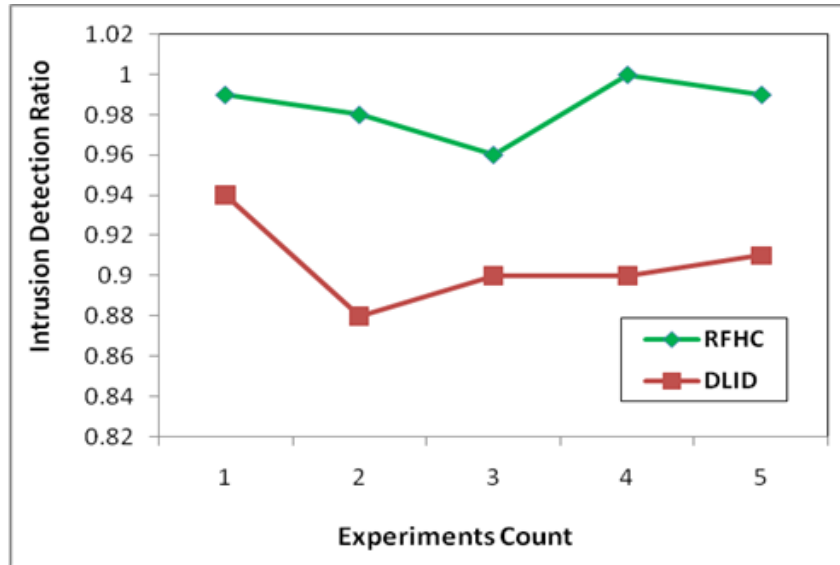


Figure 3. RFHC and DLID mechanisms for DoS intrusion detection ratio

Generally, the intrusion detection ratio is minimized by raising the intrusion count. However, the proposed RFHC mechanism increases the detection ratio since it applies an RF algorithm to detect the intrusion efficiently. The existing DLID mechanism provides a lesser detection ratio than an RFHC mechanism. In addition, the DLID mechanism does not use the optimal search algorithm, but the proposed mechanism uses the hill climbing method to select the best feature.

Alternatively, to ensure the efficiency of the model, the RFHC mechanism is employed. Figure 4 displays the results, like precision, recall, and accuracy of RFHC and DLID mechanisms. These three metrics show the network performance. This figure clearly says that the proposed RFHC mechanism presents a ratio of 0.99 precision, 0.996 accuracy, and 0.98 recall ratio by applying the RF algorithm. However, the existing DLID mechanism using the DL algorithm has a lesser precision ratio, recall ratio, and accuracy ratio.

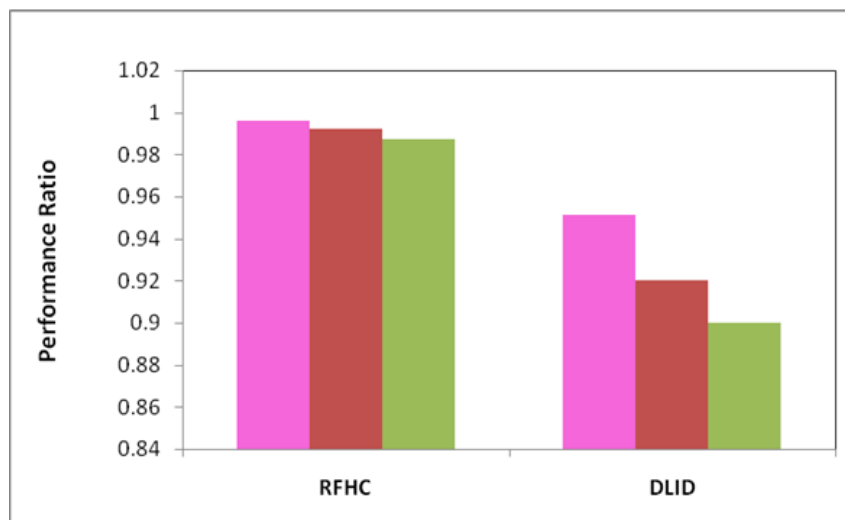


Figure 4. RFHC and DLID mechanisms for performance evaluation ratio

### 5. CONCLUSION

Detection of Intrusion is a recent knowledge that has enhanced cloud security. Recently, machine learning algorithms have been used to improve safety and supervise systems efficiently. In this article, we present a RF algorithm with a hill-climbing algorithm to enhance intrusion detection at the endpoint and

network for detecting intrusions. This mechanism uses a hill-climbing algorithm that selects the best feature, so it minimizes the execution time and unrelated data from the database. The RF algorithm separates the intrusion from normal in the cloud system. Experimental outcomes exposed that the RFHC mechanism raised the intrusion detection ratio and diminished the miss detection ratio. Additionally, it improved the precision, recall, and accuracy of the cloud system. In the future, we will apply ensemble learning to detect multiple attacks and equate the cloud system load.

## REFERENCES





- [1] M. Goudarzi, S. Ilager, and R. Buyya, "Cloud computing and internet of things: recent trends and directions," in *Internet of Things*, 2022, pp. 3–29.
- [2] P. J. Sun, "Security and privacy protection in cloud computing: discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, p. 102642, Jun. 2020, doi: 10.1016/j.jnca.2020.102642.
- [3] S. Shamsirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, "Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues," *Journal of Information Security and Applications*, vol. 55, p. 102582, Dec. 2020, doi: 10.1016/j.jisa.2020.102582.
- [4] V. Chang *et al.*, "A survey on intrusion detection systems for fog and cloud computing," *Future Internet*, vol. 14, no. 3, p. 89, Mar. 2022, doi: 10.3390/fi14030089.
- [5] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint detection & response: a malware identification solution," in *2021 International Conference on Cyber Warfare and Security, ICCWS 2021 - Proceedings*, Nov. 2021, pp. 1–8, doi: 10.1109/ICCWS53234.2021.9703010.
- [6] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
- [7] J. F. C. 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.
- [8] P. Rana *et al.*, "Intrusion detection systems in cloud computing paradigm: analysis and overview," *Complexity*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/3999039.
- [9] M. Bakro *et al.*, "Efficient intrusion detection system in the cloud using fusion feature selection approaches and an ensemble classifier," *Electronics (Switzerland)*, vol. 12, no. 11, p. 2427, May 2023, doi: 10.3390/electronics12112427.
- [10] C.-C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *2010 39th International Conference on Parallel Processing Workshops*, Sep. 2010, pp. 280–284, doi: 10.1109/ICPPW.2010.46.
- [11] G. Prashanth, V. Prashanth, P. Jayashree, and N. Srinivasan, "Using random forests for network-based anomaly detection at active routers," in *2008 International Conference on Signal Processing, Communications and Networking*, 2008, pp. 93–96, doi: 10.1109/ICSCN.2008.4447167.
- [12] S. D. D. Anton, S. Sinha, and H. D. Schotten, "Anomaly-based intrusion detection in industrial data with SVM and random forests," in *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sep. 2019, pp. 1–6, doi: 10.23919/SOFTCOM.2019.8903672.
- [13] M. Kopp, T. Pevný, and M. Holeňa, "Anomaly explanation with random forests," *Expert Systems with Applications*, vol. 149, p. 113187, Jul. 2020, doi: 10.1016/j.eswa.2020.113187.
- [14] N. Aslam *et al.*, "Anomaly detection using explainable random forest for the prediction of undesirable events in oil wells," *Applied Computational Intelligence and Soft Computing*, vol. 2022, pp. 1–14, Aug. 2022, doi: 10.1155/2022/1558381.
- [15] M. R. Y. M. and D. U. B. Mahadevaswamy, "Energy efficient routing in wireless sensor network based on mobile sink guided by stochastic hill climbing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, p. 5965, Dec. 2020, doi: 10.11591/ijece.v10i6.pp5965-5973.
- [16] S. Sakamoto, E. Kulla, T. Oda, M. Ikeda, L. Barolli, and F. Xhafa, "A comparison study of hill climbing, simulated annealing and genetic algorithm for node placement problem in WMNs," *Journal of High Speed Networks*, vol. 20, no. 1, pp. 55–66, 2014, doi: 10.3233/JHS-140487.
- [17] X. Ma, X. Fu, B. Luo, X. Du, and M. Guizani, "A design of firewall based on feedback of intrusion detection system in cloud environment," in *Proceedings - IEEE Global Communications Conference, GLOBECOM*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013771.
- [18] T. Lenard and R. Bolboaca, "A statefull firewall and intrusion detection system enforced with secure logging for controller area network," in *ACM International Conference Proceeding Series*, Nov. 2021, pp. 39–45, doi: 10.1145/3487405.3487650.
- [19] P. Singh and V. Ranga, "Attack and intrusion detection in cloud computing using an ensemble learning approach," *International Journal of Information Technology (Singapore)*, vol. 13, no. 2, pp. 565–571, Apr. 2021, doi: 10.1007/s41870-020-00583-w.
- [20] A.-R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *Journal of Cloud Computing*, vol. 12, no. 1, p. 127, Aug. 2023, doi: 10.1186/s13677-023-00491-x.
- [21] S. Krishnaveni, S. Sivamohan, S. S. Sridhar, and S. Prabakaran, "Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing," *Cluster Computing*, vol. 24, no. 3, pp. 1761–1779, Sep. 2021, doi: 10.1007/s10586-020-03222-y.
- [22] M. Rajmohan, C. Srinivasan, O. R. Babu, S. Murugan, and B. S. K. Reddy, "Efficient Indian sign language interpreter for hearing impaired," in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Aug. 2023, pp. 914–917, doi: 10.1109/SmartTechCon57526.2023.10391782.
- [23] B. Meenakshi, B. Gopi, L. Ramalingam, A. Vanathi, S. Sangeetha, and S. Murugan, "Wireless sensor networks for disaster management and emergency response using SVM classifier," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 647–651, doi: 10.1109/SmartTechCon57526.2023.10391435.







- [24] T. Meenakshi, R. Ramani, A. Karthikeyan, N. S. Vanitha, and S. Murugan, "Power quality monitoring of a photovoltaic system through IoT," in *International Conference on Sustainable Communication Networks and Application, ICSCNA 2023 - Proceedings*, Nov. 2023, pp. 413–418, doi: 10.1109/ICSCNA58489.2023.10370494.
- [25] R. Raman, V. Sujatha, C. Bhupeshbhai Thacker, K. Bikram, M. B. Sahaai, and S. Murugan, "Intelligent parking management systems using IoT and machine learning techniques for real-time space availability estimation," in *International Conference on Sustainable Communication Networks and Application, ICSCNA 2023 - Proceedings*, Nov. 2023, pp. 286–291, doi: 10.1109/ICSCNA58489.2023.10370636.
- [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 (IJECS)*, 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 (IJECE)*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.

## BIOGRAPHIES OF AUTHORS







**Mr. Satheesh Kumar 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. He extensive background includes a strong focus on Data and Cloud projects, where his excelled in system analysis, requirement gathering, design, development, testing, quality assurance, implementation, and support across banking, insurance, health care, 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 exhibit 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 my expertise in data movement. Furthermore, my background encompasses reengineering legacy applications into microservices on the Databricks platform and executing successful Teradata to Snowflake migrations & Teradata to GCP Big Query. 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: satheeshkumarsekar12@yahoo.com.






**Mr. Palaniraj Rajidurai Parvathy**     is a project manager at Mphasis Corporation in Chandler, Arizona, USA. He has 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, Altreyx, Xceptor (RPA)). Rewarded from Customer for providing "Customer Value Addition" for Performance tuning on Schedule. He has been rewarded the "Star Performer" Award of the Quarter for a Support Project by Hexaware Leadership. Also, he received the "Stat Performer" Award of the Quarter for Migration Project from Hexaware Leadership. Moreover, rewarded "most valuable player" support project from Wipro- Best Buy Account Leadership. Furthermore, rewarded a "Feather in my cap" for outstanding contribution to the project Business Group Hierarchy Iteration. He was rewarded with a "Feather in my cap" award for his outstanding contribution to Project Business Group Hierarchy Iteration 1. He can be contacted at email: palaniraj18@gmail.com.






**Dr. Latika Pinjarkar**     has obtained her Ph.D. in Computer Science and Engineering from CSVTU CG, India in 2019. She completed an M.Tech degree in Computer Technology and Application from CSVTU, CG, India in 2008 and a BE degree in Computer Technology from Nagpur University, MH in 1999. She has been engaged in research and teaching for more than 22 years. At present, she is an Associate Professor and Academic Head in the CSE Department at Symbiosis Institute of Technology Nagpur, Symbiosis International (Deemed University) Pune, MH, India. She has presented more than 40 papers in International/National Journals/ Conferences and has 05 Patents to her credit. She has completed one research project sponsored by TEQIP-III. Her research interests include Image Processing, Computer Vision, Content-Based Image Retrieval (CBIR) and Machine Learning. She can be contact at email: latika.pinjarkar@sitnagpur.siu.edu.in.








**Dr. Raman Latha**    received the Ph.D. degree in CSE from PMU, Thanjavur in March 2017 and the M.Tech. degree in Computer science and Engineering from the Anna University, TN, India, in 2009 and the Bachelor degree in computer application from Madras University, TN, India, 2004. Her research interests include Wireless Sensor Networks, Machine learning and Networks. She has published 35 research papers in various International Journals and conferences. Presently she is working as professor in the department of CSE, K. Ramakrishnan College of Engineering, Trichirapalli, TN, 600028. She can be contact at email: lathait64@gmail.com.






**Mr. Mani Sathish**    is working as an Assistant professor in the department of computer science and engineering at Chennai Institute of Technology, Kandrathur, Chennai. He is having rich experience in teaching more than 10 years in reputed institutions. He is an awesome researcher too in the field of artificial intelligence, deep learning and image processing. To his credit, he has published many research articles in well reputed journals and filed Patents also. He can be contact at email: sathishm@citchennai.net.



**Dr. Munnangi Koti Reddy**    received the Ph.D. Degree in ECE from KU, Raipur in January 2019 and the M.Tech. degree in VLSI Design from the Viganan University, AP, India, in 2011 and the B.Tech. degree in Electronics and Communication Engineering from JNTU Kakinada, A.P, India, in 2009 and Diploma in ECE from Gudlavalleru Engineering College. His research interests include wireless communications, embeded systems and vlsi design. He has published 12 research papers in various International Journals and conferences. Presently he is working as Associate professor in the department of ECE, Universal College of Engineering and Technology, Guntur, AP, 522438. He can be contacted at email: kotiuacet@gmail.com.



**Mr. 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.