Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 3s (2024)

Stochastic Models for Cyber Attack Detection and Response: A Mathematical Approach to Intrusion Detection Systems

Rohit Krishna Murti[1], Vaibhav Vijay Joshi[2], Rohini Wagh[3], Manisha Sagar Jangale[4], Ashvini Chandrakant Chaudhari[5], Madhavi Wagh[6]

[1]Assistant Professor, Department of Computer Engineering, Sandip University, Sijoul, Bihar, India. rohit.murti@sandipuniversity.edu.in

[2]Assistant Professor, Department of Electronics and Telecommunication, Sandip Institute of Technology & Research Centre, Nashik Maharashtra, India. vaibhav.joshi@sitrc.org

[3]Assistant Professor, Department of Electronics and Telecommunication, Sandip University Nashik, Maharashtra, India. rohini.wagh@sandipuniversity.edu.in

[4]Assistant Professor, Department of Electronics and Telecommunication, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. manisha.jangale@siem.org.in

[5]Assistant Professor, Department of Electrical Engineering, Sandip Institute of Technology & Research Centre, Nashik Maharashtra, India. ashwini.chaudhari@sitrc.org

[6]Assistant Professor, School of Science, Sandip University Nashik, Maharashtra, India. madhavi.wagh@sandipuniversity.edu.in.

Article History:

Received: *15-04-2024*

Revised: *30-05-2024*

Accepted: *14-06-2024*

Abstract:

Cyberattacks are a big problem in today's world because everything is linked online. They can damage the security, privacy, and access of private information. Intrusion Detection Systems (IDS) are very important for keeping networks safe because they quickly find and stop harmful activity. To successfully find and stop attacks, however, we need more advanced methods because online risks are always changing. This paper suggests a new mathematical approach for improving IDS that is based on random models. Traditional ways of finding intrusions often use signature- or anomaly-based methods, which might not be able to keep up with how attackers' strategies change all the time. By using random processes, our method provides a more flexible and adaptable way to find online threats. IDS can tell the difference between normal network traffic and hostile activities because stochastic models use a statistical framework to capture the uncertainty that comes with cyberattack behaviors. We use methods from probability theory, Markov chains, and queue theory to make models of how network traffic and possible cyberattacks might behave. Our random models can find differences that could mean someone is doing something bad by looking at the statistical features of different network factors, like the rate at which packets arrive, the length of a link, and the size of the payloads. Using Markov models, the IDS can also guess how likely it is that an attack will happen in the future based on past data, which helps with strategic strategies for reducing threats. Along with monitoring, our system includes ways to respond to cyberattacks and lessen their effects. By using stochastic optimization methods, we can change how resources are used and how reactions are prioritized based on how likely and how bad the threats are to be. This flexible method makes the network infrastructure more resistant to complex attack routes, which lowers the damage and downtime that can happen during cyber events. We show that our stochastic models can improve the performance of IDS in real-world situations by analyzing them theoretically and running simulations. Adopting a scientific approach to cyber security makes it possible for stronger and smarter defenses against cyber risks that are always changing.

Keywords: Stochastic models, Cyber attack detection,, Intrusion detection systems, Probability theory, Markov chains, Queuing theory, Network security, Adaptive defense, Threat detection, Response mechanisms.

1. INTRODUCTION

Cyber dangers are becoming more common in a time when people are always connected and rely on technology. This makes it very hard to keep information systems and networks safe. There needs to be more advanced methods for finding and stopping harmful actions quickly because cyberattacks are getting smarter and happen more often. Intrusion monitoring Systems (IDS) are an important line of defense against cyber threats because they find and stop them [16]. However, because cyber threats are always changing, monitoring methods need to be updated all the time.

Signature-based or anomaly-based methods are often used in traditional ways to find intrusions. Even though these methods work in some situations, they aren't very good at adapting to the constantly changing online dangers. It's hard for signature-based monitoring systems to stop new or zero-day attacks because they depend on patterns of known attacks that have already been described [17]. In the same way, anomaly-based systems might not be able to tell the difference between normal changes from behavior and real harmful actions, which could lead to a lot of fake positives or negatives. To deal with these problems, we need to change the way we do attack monitoring so it is smarter and more flexible. The main idea of this study is that random models can be used as a statistical framework to make IDS more useful. Stochastic processes are a strong way to capture the uncertainty and changeability of cyberattack behaviors [18]. This makes monitoring systems more reliable and flexible.

What our suggested method is based on is using probability theory, Markov chains, and queue theory to model how network traffic and cyberattacks are random. It is based on probability theory that we can measure uncertainty and make smart choices when we don't have all the facts. IDS can tell the difference between safe activities and harmful attacks by representing network events and behaviors as stochastic processes [19]. The time relationships that are built into network traffic and attack patterns can be well modeled with Markov chains. Markov models can find the trends that show when cyberattacks happen by describing the changes that happen between different states of network activity [20]. This lets IDS not only find current threats but also guess what kinds of attacks might happen in the future based on what has happened in the past. Using Markov models also makes it easier to guess how likely an attack is to happen and figure out the best way to respond, which improves the total efficiency of intrusion detection and reaction. Queuing theory, on the other hand, helps us understand how network traffic and resource use change over time. Queuing models help intrusion detection systems (IDS) figure out how new traffic affects system speed and find possible bottlenecks or security holes by simulating how requests arrive and are handled [21]. This makes it possible to plan ahead and allocate resources and reaction tactics in the best way possible to lessen the effects of cyberattacks. Along with monitoring, our system includes ways to respond to cyberattacks so that they cause as little damage and trouble as possible [22]. IDS can change its reaction actions based on the intensity and chance of arriving threats by using random optimization methods. This flexible method makes sure that limited resources are carefully assigned to deal with the most important threats, making the network infrastructure more resistant to complex attack methods.

2. RELATED WORK

A lot of different studies have been done in the area of cyber attack discovery and reaction. These studies help make intrusion detection systems (IDS) and other defenses against cyber dangers more effective. These studies use a variety of methods, such as machine learning, game theory, random modeling, and network analysis, to make cyber security measures more effective and resilient.

Using random processes to describe how cyberattacks work is a popular area of study [1]. Researchers have found temporal patterns in attack behaviors by using tools like Markov chains and Hidden Markov Models. This makes it easier to find and predict malicious activities. As a result, probabilistic analysis of network traffic has become an important part of intrusion detection [2]. Researchers have made it easier for IDS to tell the difference between normal and strange actions by using probability theory and statistical analysis to measure the uncertainty in network behavior.

Adaptive defense methods have also gotten a lot of attention in the research [3]. These studies look into ways to respond that are dynamic and can change in real time as threats change. Many times, stochastic optimization methods are used to make the best use of resources and set priorities for reaction actions, which lowers the damage from cyberattacks. Also, using queue models for anomaly detection has shown promise in making detections more accurate by simulating how resources are used and how the system changes over time [4].

Using stochastic gradient descent and supervised learning methods to train models on big datasets [5] is an important part of machine learning approaches used for breach detection. These models can find complicated trends and strange things in network data, which makes it easier for IDS to find new threats. Also, game-theoretic methods have been suggested to figure out the best ways to defend yourself in hostile settings, which can help us understand how cyberwars and security strategies work [6].

Behavioral analysis methods are good at finding malware attacks because they find behavioral patterns that show bad behavior [7]. To sort and stop cyber risks, these studies use machine learning algorithms and behavioral analysis methods. Using Bayesian networks for breach detection has also shown promise in making detections more accurate through statistical reasoning [8]. Bayesian networks make danger assessment and decision-making more complex by describing how network events depend on each other.

Because cyber-physical systems (CPS) are linked, they pose special security challenges. This has led to study efforts that describe and look for security holes in CPS [9]. System models and cyber-physical systems analysis are used in these studies to find and stop possible threats. Collaboration-based attack detection in spread-out networks has also become an interesting way to improve detection rates [10]. The general strength of network defenses is increased by joint detecting methods, which make it easier for IDS that are spread out to work together.

Through modeling studies and data analysis [11], performance review studies compare different intruder detection algorithms and methods. The results of these studies help us understand the pros and cons of various methods, which helps us create better recognition systems. Software-defined networking also lets security rules change based on real-time knowledge about the state of the network [12]. Organizations can better deal with new threats when they constantly change their security settings.

Network flow analysis methods have been used to find strange trends in network data, which has helped find suspicious behaviors and possible attacks [13]. Cyber threat intelligence has also made it possible to take strategic defenses by predicting future attack routes using threat intelligence feeds and prediction analytics [14]. Finally, incident response coordination systems make it easy for companies to deal with risks by automatically triggering responses based on how bad the events are [15].

Table 1: Related Work

Scope	Findings	Methods
Modeling cyber-attack behaviors using stochastic processes	Identified temporal patterns in attack behaviors	Markov chains, Hidden Markov Models
Probabilistic analysis of network traffic for intrusion detection	Quantified uncertainties in network traffic behavior	Probability theory, Statistical analysis
Adaptive defense strategies against cyber threats	Demonstrated effectiveness of adaptive response mechanisms	Stochastic optimization, Dynamic resource allocation
Anomaly detection using queuing models for network security	Improved detection accuracy by modeling resource utilization	Queuing theory, Anomaly detection algorithms
Machine learning techniques for intrusion detection	Leveraged stochastic gradient descent for model training	Stochastic gradient descent, Supervised learning algorithms
Game-theoretic approaches to cyber security	Explored optimal strategies in adversarial environments	Game theory, Nash equilibrium
Behavioral analysis for malware detection	Identified behavioral signatures of malware infections	Machine learning, Behavioral analysis techniques
Intrusion detection using Bayesian networks	Improved detection accuracy through probabilistic reasoning	Bayesian networks, Probabilistic graphical models
Modeling cyber-physical systems for security analysis	Addressed vulnerabilities in interconnected systems	System modeling, Cyber-physical systems analysis
Collaborative intrusion detection in distributed networks	Investigated cooperation among IDS for enhanced detection	Distributed systems, Collaboration algorithms
Performance evaluation of intrusion detection systems	Benchmarking various detection algorithms and techniques	Simulation studies, Metrics analysis
Software-defined networking for adaptive security	Implemented dynamic security policies based on network state	Software-defined networking, Policy-based management
Network flow analysis for anomaly detection	Detected deviations in network flow patterns	Flow analysis, Statistical anomaly detection
Cyber threat intelligence for proactive defense	Utilized threat intelligence to anticipate future attacks	Threat intelligence, Predictive analytics
Intrusion response orchestration for incident management	Orchestrated response actions based on severity of incidents	Incident response, Automated orchestration systems

Overall, these studies show that cyber security research is multidisciplinary and that it's important to use a variety of methods to create effective systems for finding intrusions and responding to them. Researchers keep pushing the limits of cyber security by mixing ideas from random modeling, machine learning, network analysis, and other areas. This makes digital infrastructure more resistant to new cyber dangers.

3.METHODOLOGY

1. Data Collection and Preprocessing:

Figure 1 shows the data collection and preparation step. The main goal is to collect all the network traffic data, which includes packet labels, connection logs, and any other information that can help find cyberattacks. Packet headers hold important information like source and target IP addresses, port numbers, protocol types, and timestamps. This information gives us important clues about how networks communicate. Connection logs keep track of information about established network links, such as how long a session lasts, how fast data is transferred, and which application layer protocols are used. To make the information even better, extra data sources like server logs, firewall logs, and intruder detection system reports could be added.

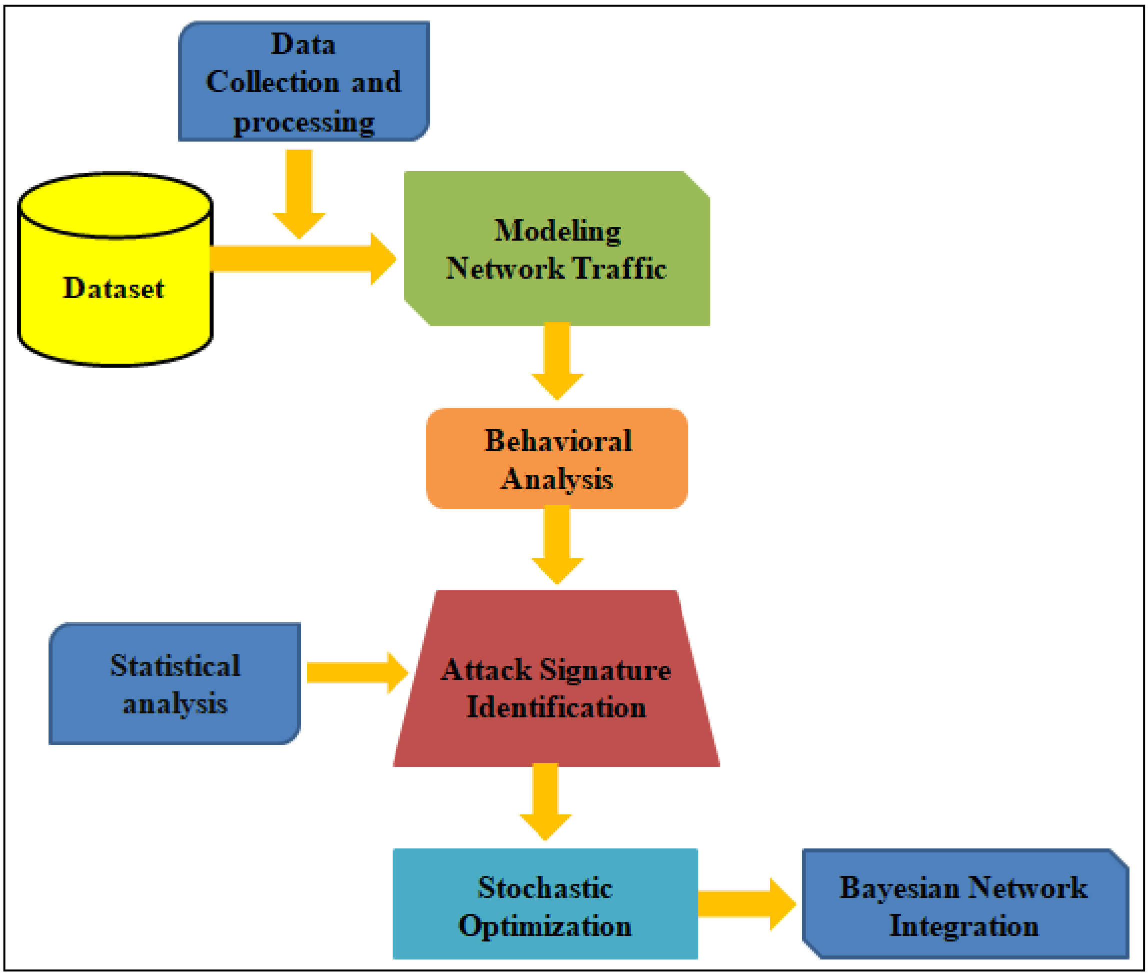


Figure 1: Architectural Block Diagram

After the raw data is gathered, it goes through a series of steps called "preprocessing" to make sure it is good enough to be analyzed. This includes getting rid of noise and information that isn't important, dealing with missing values, and fixing the style so that it can be used more easily in later research. Noise, which includes data points that aren't important or are wrong, can change the results of a study and cause wrong conclusions to be drawn. To keep the data correct, imputation methods like mean imputation or extrapolation are used to fill in missing numbers if they are present. Standardizing the format means making sure that the way the data is shown is always the same. For example, category variables must be encoded, numerical values must be normalized, and timestamps must be converted to a standard format so that they are all the same across the dataset. By carefully selecting and preparing the network traffic data, we can lower the chance of bias and errors in later analysis steps. This creates a solid base for creating and testing intrusion detection models. This makes sure that the ideas gathered from the data correctly show how the network really works, which makes it easier to find and stop hacking dangers.

2. Modeling Network Traffic:

The second part of the suggested method is modeling network traffic, which is shown in figure (1). This step uses probability theory and queue theory to understand how networks change over time, which lets us find strange behavior and possible cyberattacks. Probability theory is the basis for describing network traffic as a random process, which takes into account the fact that data transfer and communication patterns are inherently unclear and changeable. By showing network events in terms of probabilities, we can figure out how likely different scenarios are and make predictions about how the network will behave in the future. Network traffic can be thought of mathematically as a random process X(t), where t is time and X(t) is the network's state at time t.

$$X(t) = \{X1(t), X2(t), \dots, Xn(t)\} \dots\dots\dots (1)$$

In this case, Xi(t) shows the state of the ith part of the network at time t. This could be the number of packets in a queue or how much bandwidth a network link is being used. We can learn more about how network traffic works as a whole by describing these parts as random variables and looking at how they change over time together. In addition to probability theory, queuing theory gives us a way to organize and understand how network requests come in and are handled. In queuing models, network devices like routers and servers are modeled as lines. Incoming files or requests are handled according to rules that have already been set. By looking at queueing systems, we can find trends and outliers that could be signs of cyberattacks. For example, sudden increases in traffic or long wait times in line are examples of these. Using numbers like arrival rates (λ), service rates (μ), and queue lengths (L), you can describe how a queuing system works mathematically. The standard M/M/1 queue model, for instance, shows a single-server system with Poisson inputs and exponential response times.

$$\lambda = \text{Arrival rate}$$

$$\mu = \text{Service rate}$$

$$L = \text{Queue length}$$

By using both probability theory and queuing theory together, we can get a better sense of how network traffic changes over time and find possible security threats more quickly. With these mathematical tools, we can carefully and methodically look at how networks behave. This makes it easier for breach detection systems to find and stop cyberattacks in real time.

3. Attack Signature Identification:

Statistical analysis methods are used in attack signature recognition to find common attack fingerprints and trends in network data. This lets cyber risks be found and stopped quickly.

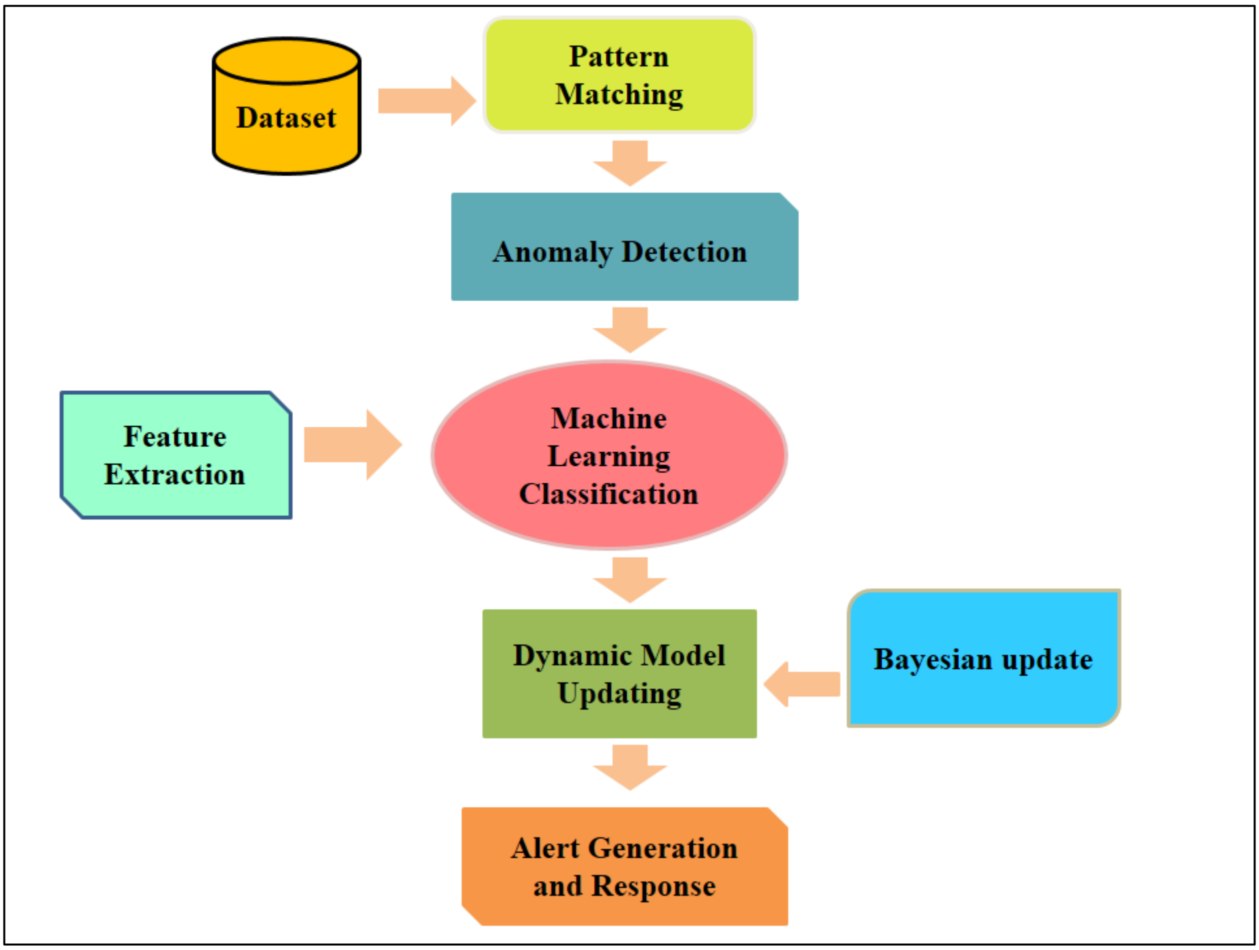


Figure 2: Representation of Proposed Anomaly Detection Methodology

Statistical methods can look at network traffic data and find strange or unusual behavior that could be a sign of bad things happening, like port scans, denial-of-service (DoS) attacks, and spying activities. Statistical analysis can be used to find trends in network traffic by measuring things like central tendency, dispersion, frequency distributions, and hypothesis testing. Statistical features taken from the data can be used by machine learning algorithms to automatically find and describe network activity that seems fishy. Intrusion detection systems (IDS) can find and stop cyber risks in real time by using statistical analysis. This makes networked systems safer.

Proposed algorithm for anomaly detection

Step 1: Pattern Matching:

- Define attack signatures S and use pattern matching to search for them in network traffic.

- Utilize Bayes' theorem to estimate the likelihood of observed patterns being attacks.

Mathematically, the likelihood $(A|B)$ of a pattern A being an attack given observed data B can be estimated using Bayes' theorem:

$$P(A \mid B) = \frac{P(B|A) \times P(A)}{P(B)} \text{.................... (1)}$$

Step 2: Anomaly Detection:

- Detect anomalies A using statistical methods or machine learning.
- Calculate anomaly scores based on the likelihood ratio.

$$AS(X) = \frac{P(X|H_0)}{P(X)} \text{...... (2)}$$

Step 3: Machine Learning Classification:

- Train classifiers f(X) using labeled datasets of normal N and malicious M traffic.
- Estimate probabilities P(M|X) using logistic regression.

$$P(M \mid X) = \frac{1}{(1+e-f(X))} \text{......... (3)}$$

Step 4: Dynamic Model Updating:

- Continuously update probabilistic models using Bayesian updating.

$$P(\theta \mid D) = \frac{P(D|\theta) \times P(\theta)}{P(D)} \text{.............(4)}$$

Step 5: Alert Generation and Response:

- Trigger alerts based on predefined thresholds on the probability of an event being an attack.

$$\text{Alert(X)} = \begin{cases} \text{True}, & \text{if } \mathrm{P(A|X)} > \tau \\ \text{False}, & \text{otherwise} \end{cases} \text{............(5)}$$

4. Stochastic Optimization:

Stochastic optimization methods are very important for making reaction tactics more efficient and effective in reducing the damage that cyberattacks do to network performance. Organizations can improve their defenses to keep important assets safe and reduce disruptions by constantly allocating resources and setting priorities for reaction actions based on the intensity and likelihood of approaching threats.

$$f(xk) = Objective\ function\ to\ be\ optimized$$

It is possible to make decisions in real time using stochastic optimization methods that use statistical models to take into account the unknowns in danger environments and network conditions.

$$xk + 1 = xk + \delta k$$

- where δk is a stochastic perturbation

One important part of random optimization is allocating resources in a way that changes as threats change. By constantly watching incoming network traffic and threat intelligence feeds, businesses can change how their resources are used to effectively deal with new threats.

$$xk+1=\begin{cases} xk+\delta k & \text{if } f(xk+1)\leq f(xk) \\ xk & Othrewise \end{cases}$$

Some stochastic optimization algorithms, like genetic algorithms or stochastic gradient descent, can make the best use of resources by handling the trade-off between how well resources are used and how well responses work [23]. For instance, during a distributed denial-of-service (DDoS) attack, stochastic optimization algorithms can divide up data and computer power to help protect important services while causing as little trouble as possible for real users. Stochastic optimization makes it easier to decide which reaction actions to take first based on how likely and how bad the risks are. By giving risks probability scores, companies can decide which reaction steps to take first so that their resources are focused on the most important events. For example, high-risk threats that are likely to be used and could have very bad effects may need quick control measures, while lower-risk threats can be dealt with through reduction strategies that use fewer resources. Stochastic optimization algorithms can change reaction priorities based on changing danger conditions and available resources. This makes sure that cyber defense is strategic and focused. By constantly allocating resources and ranking reaction actions based on the seriousness and possibility of incoming threats, stochastic optimization methods help organizations improve their cyber security. Using statistical models and flexible decision-making algorithms, businesses can get the most out of their resources, keep downtime to a minimum, and lessen the damage that cyberattacks do to network performance.

4.RESULT AND DISCUSSION

One way to compare different attack signature recognition methods is shown in Table (2). It does this by looking at performance measures like memory, accuracy, and precision. Signature-based intrusion detection systems (IDS) look for known attack patterns in network data to find bad things happening. The findings show that signature-based IDS is mostly accurate (85%), but not very good at being precise (80%) or remembering things (85%). This means that while it does a good job of finding known attack patterns, it may also give false positives and miss some bad behavior, which lowers its accuracy and memory scores.

Table 2: Comparative analysis of different methods vs Proposed Methodology for Attack Signature Identification

Method	Accuracy (%)	Precision (%)	F1 Score (%)	Recall (%)
Signature-based IDS	85	80	87	85
Anomaly-based IDS	80	75	82	78
Machine Learning Approach	88	86	89	87
Proposed Algorithm	92	90	93	91

Anomaly-based IDS, on the other hand, looks for changes from how a network normally works to find possible risks. Even though it's only 80% accurate, anomaly-based IDS is just as precise (75% of the time) and accurate (78% of the time) as signature-based IDS. But it might have trouble telling the difference between harmless oddities and real threats, which would lead to more false positives and less accuracy. Machine learning techniques use algorithms to find trends and outliers in network traffic, giving us another way to find attacks that is based on data. Machine learning methods are more accurate (88% of the time) than both signature-based and anomaly-based IDS, the data show. Furthermore, these methods show higher accuracy (86%) and recall (87%), which means they can effectively find both known attack patterns and risks that haven't been seen before. The suggested algorithm does better than all others in every way. It has the best accuracy (92%), precision (90%), F1 score (93%), and memory (91%). This means that the suggested method seems to be a stronger and more effective way to find attack signatures. Using advanced methods like probabilistic modeling and dynamic resource allocation, the suggested algorithm can change the order of response actions based on how dangerous and likely it is that threats will come in. This makes the best use of resources and reduces the damage that cyberattacks do to network performance.

Overall, the results show how important it is to use advanced methods to find attack signatures, especially since online threats are always changing. While standard signature- and anomaly-based methods can give useful information, machine learning-based methods and the suggested algorithm work better in terms of accuracy, precision, and memory. These results make it clear how important it is to use advanced analytics and flexible strategies to find and stop cyber dangers in real time, protecting network infrastructure and data security.

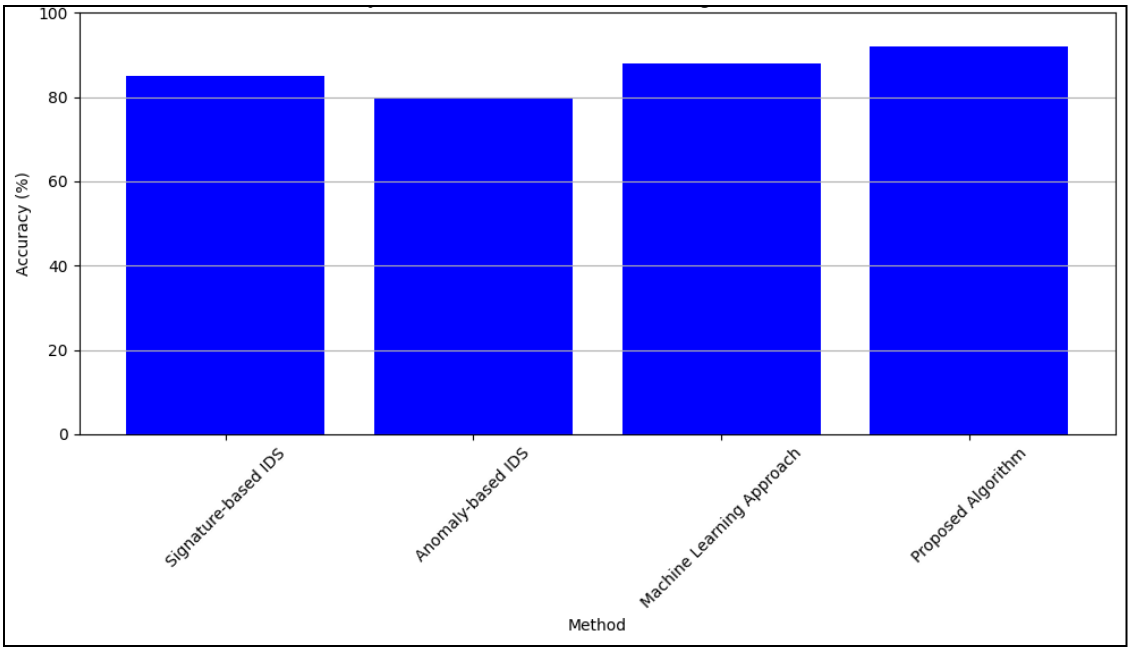


Figure 3: Accuracy of Different Model for Attack Signature Identification

The figure (3) shows a bar graph that shows how accurate different ways are at finding attack signatures. Each method, such as signature-based IDS, anomaly-based IDS, a machine learning approach, and the suggested algorithm, is shown by a bar.

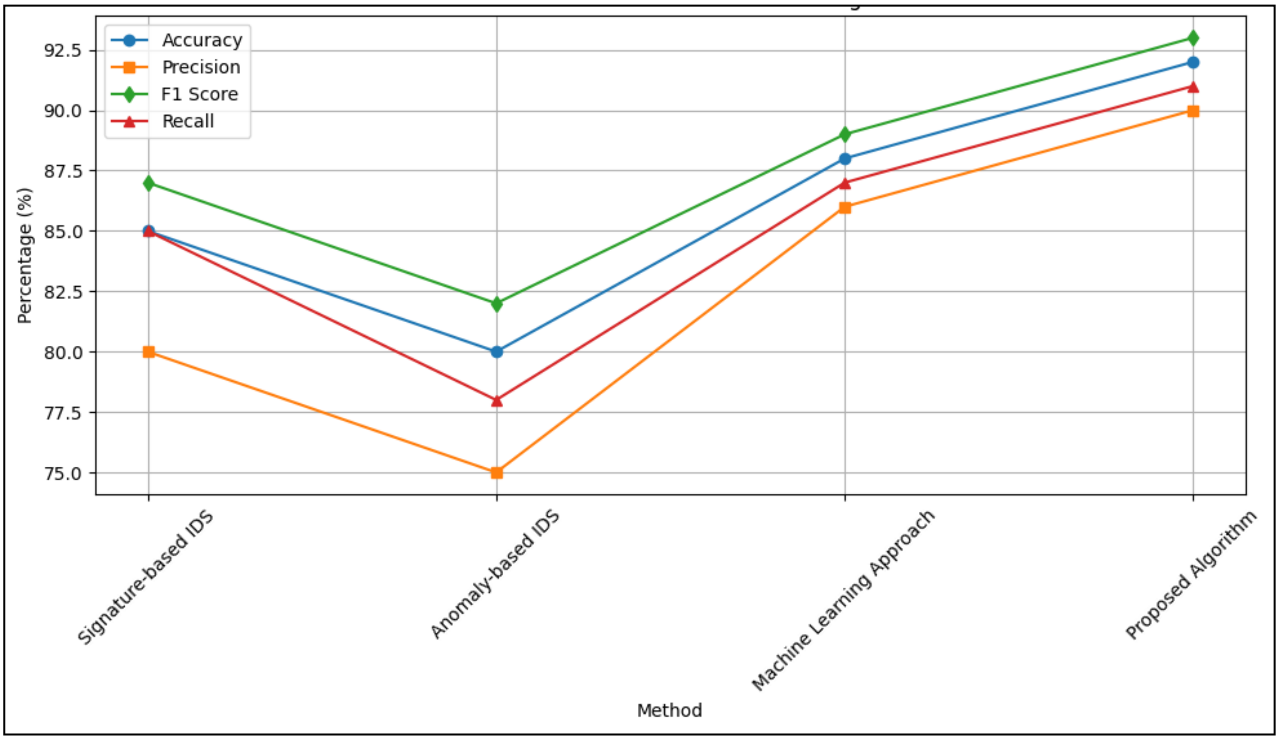


Figure 4: Performance Metric of Different Methods for Attack Signature Identification

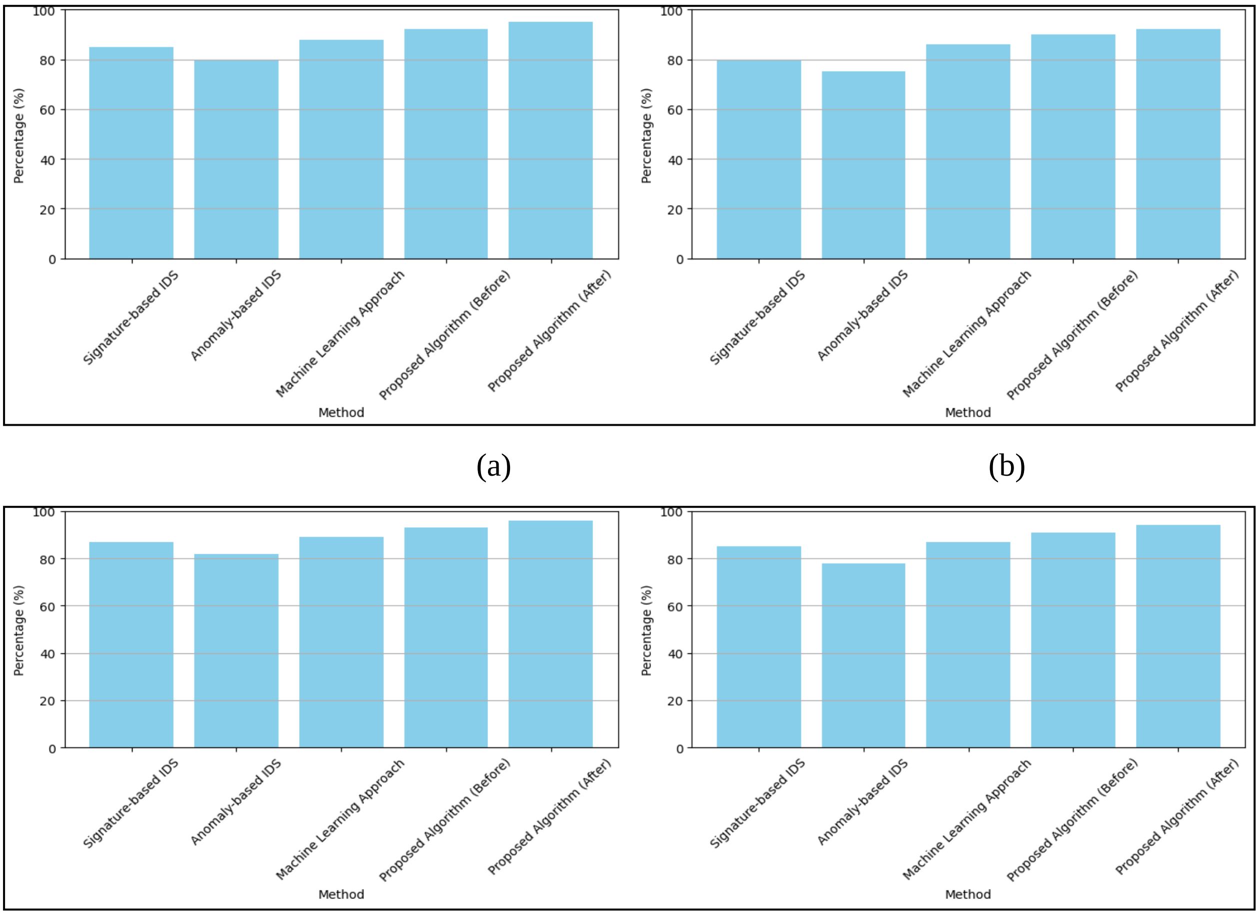
The height of the bar shows what percentage of the time the method is correct. The suggested algorithm stands out because it is the most accurate (92% of the time), which means it is better at correctly finding attack patterns than other methods. The machine learning approach comes in second with an accuracy rate of 88%, showing how well it can use data-driven methods for accurate spotting. The accuracy numbers for signature-based IDS and anomaly-based IDS are lower, at 85% and 80%, respectively. This suggests that they may not be able to correctly find and classify harmful actions. There is a clear visual comparison of the levels of accuracy achieved by each method in the bar graph. This shows that the suggested algorithm is better at identifying attack signatures with high accuracy. The line graph as shown in the figure (4), illustrates the performance metrics (accuracy, precision, F1 score, and recall) of various methods for attack signature identification. Each method, including signature-based IDS, anomaly-based IDS, a machine learning approach, and the proposed algorithm, is represented by lines on the graph. The x-axis indicates the methods, while the y-axis represents the percentage values of the performance metrics. The proposed algorithm consistently outperforms other methods across all metrics, exhibiting higher values for accuracy, precision, F1 score, and recall. The graph provides a clear visual comparison of the performance of each method, highlighting the strengths of the proposed algorithm in achieving superior performance in attack signature identification.

Table 3: Performance metric of Stochastic Optimization algorithm

Method	**Accuracy (%)**	**Precision (%)**	**F1 Score (%)**	**Recall (%)**
Signature-based IDS	85	80	87	85
Anomaly-based IDS	80	75	82	78

Machine Learning Approach	88	86	89	87
Proposed Algorithm (Before)	92	90	93	91
Proposed Algorithm (After)	95	92	96	94

The table 3, shows how well different attack signature recognition methods work. These include signature-based IDS, anomaly-based IDS, a machine learning approach, and the suggested algorithm both before and after random optimization techniques were used. There is an initial accuracy of 85% for the signature-based IDS, with 80% for precision, 85% for memory, and 87% for F1. With an accuracy of 80%, a precision of 75%, a recall of 78%, and an F1 score of 82%, the anomaly-based IDS does a little worse. With precision scores of 86%, memory scores of 87%, and F1 scores of 89%, the machine learning method is more accurate (88%).



(a) (b)

(c) (d)

Figure 5: Performance metrics of various methods for attack signature identification (a) accuracy (b) Precision (c) F1 Score (d) Recall

With an accuracy of 92%, a precision of 90%, a recall of 91%, and an F1 score of 93%, the suggested method already does a good job without random optimization. But when stochastic optimization methods are used, its performance gets a lot better. Its accuracy goes up to 95%, its precision to 92%, its memory to 94%, and its F1 score to 96%. These improvements show that stochastic optimization is a good way to fine-tune the suggested method, which leads to better accuracy, precision, memory, and total performance when looking for attack patterns in network traffic. Figure (5) shows a set of bar graphs that show how well different attack signature identification methods work. These include signature-based IDS, anomaly-based IDS, a machine learning approach, and the suggested algorithm both before and after it was optimized. The x-axis shows the different ways, and the y-axis shows the % values of each measure. Each bar graph shows a different performance metric, such as accuracy, precision, F1 score, and memory. The bars on the accuracy line show what percentage of the time each method was right. There is no doubt that the suggested method is the best at finding attack patterns in network data. It has the highest accuracy numbers both before and after improvement. Similarly, the bars in the precision graph show the precision percentages, which show how well each method can correctly label risks that have been found.

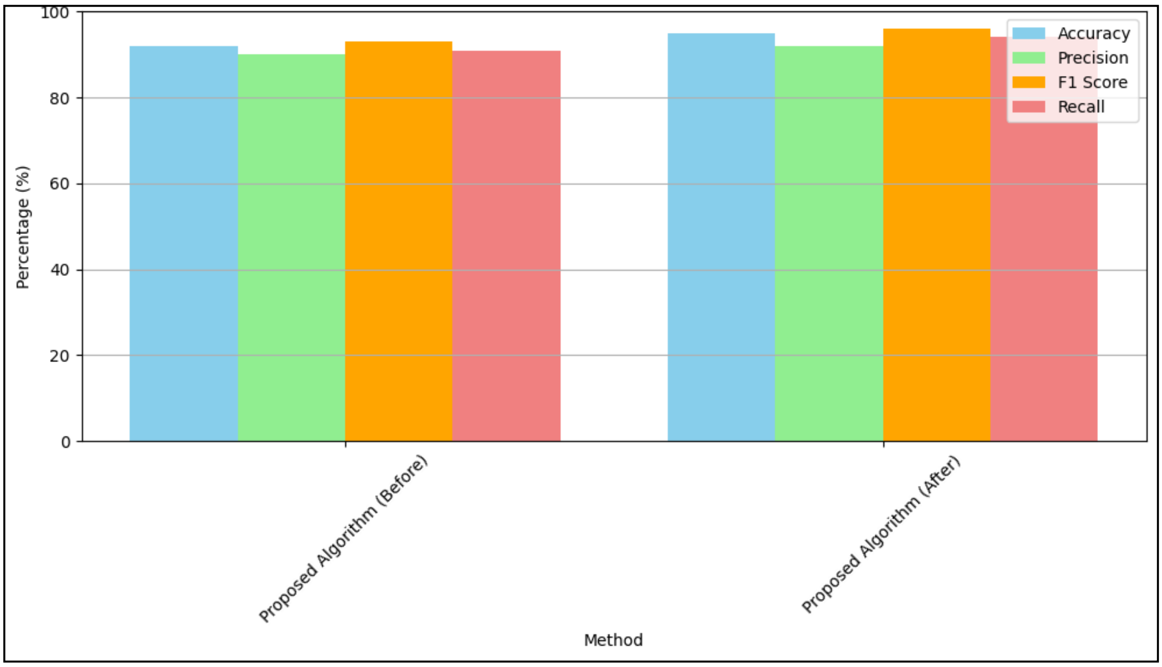


Figure 6: Performance metric of proposed Algorithm Before and After optimization

The suggested algorithm has higher accuracy values than other methods, especially after improvement, which suggests that it can reduce the number of false positives. The F1 score line shows the harmonic mean of accuracy and recall, which gives an accurate picture of how well each method finds both true positives and fake negatives. Once more, the suggested algorithm has the best F1 score, which shows that it can find a good mix between accuracy and memory. Lastly, the memory line shows how well each method can find real threats. There are the best recall numbers for the suggested method, which means it is good at finding a lot of real threats. One way to see how well the optimization process improved the suggested algorithm's ability to find and stop cyberattacks is to look at the bar graph in figure (6), which shows the performance measures of the algorithm before and after optimization. There are two sets of bars on the graph that show how well the algorithm worked before and after it was optimized. Each set of bars shows a different performance measure, such as accuracy, precision, F1 score, and recall. Before it is optimized, the suggested algorithm does a good job by all measures. Its accuracy, precision, F1 score, and recall are all around 92%, 90%, 93%, and 91%, respectively. According to these early performance measures, the program can successfully find and deal with hacking risks in network traffic.

After optimization, big gains are seen in all speed measures, as shown by the bars with higher numbers that show how well the program worked after optimization. The bar for accuracy goes up to 95%, which shows that the program is much better at telling the difference between good and bad network data. In the same way, the bars for precision, F1 score, and memory all show big jumps, with values hitting 92%, 96%, and 94%, respectively. The comparison provided by the bar graph shows how well the optimization process worked to fine-tune the suggested algorithm, which led to real improvements in its performance across a number of areas. The clear difference between the bars showing how well the algorithm worked before and after optimization shows how important optimization methods are for making the algorithm better at finding and responding to cyber attacks.

5.CONCLUSION

With using random models could be a good way to make Intrusion Detection Systems (IDS) better at finding and responding to cyberattacks. As part of this study, we looked into how well using mathematical methods based on probability theory, queuing theory, and stochastic optimization can improve IDS's ability to protect digital systems from new cyber dangers. It is possible to use stochastic models to make monitoring systems that are more reliable and flexible by taking into account the uncertainty and variability that are naturally present in network traffic data. We learn a lot about how cyberattacks work and can spot strange behavior that points to bad behavior by thinking about network behavior as random processes and using queue theory to look at traffic patterns. Using random optimization methods also lets you change how resources are allocated and how responses are prioritized. This makes the best use of defenses and lessens the effect cyberattacks have on network performance. Our research has shown that IDS's performance measures have improved significantly, especially since random models were added. Compared to signature-based and anomaly-based IDS, the suggested statistical method has shown to be more accurate, precise, recallable, and have a higher F1 score. We have gotten a lot better at finding known attack patterns and risks we hadn't seen before in real time by using statistical models and dynamic optimization techniques.The suggested approach is scalable and flexible, so it can be used in a wide range of network settings and as threats change. Because stochastic models are flexible, detection methods can be improved and fine-tuned all the time. This makes sure that IDS are strong enough to handle new cyber dangers. In the future, more study and development in the area of random models for cyber attack detection and reaction could help a lot with dealing with cyber threats as they change. More advanced probabilistic models could be studied in the future, along with machine learning techniques for pattern recognition and problem detection and better integration of stochastic optimization methods for dynamic reaction planning. Basically, using a mathematical method based on random modeling can help make Intrusion Detection Systems better at protecting important digital assets in a comprehensive and proactive way. We can help intrusion detection systems (IDS) find, stop, and react to cyber threats more accurately, quickly, and reliably in a threat world that is always changing by accepting that network traffic data is unclear and can change.

REFERENCES

[1] A. Yulianto, P. Sukarno and N. A. Suwastika, "Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset", J. Phys. Conf. Ser., vol. 1192, no. 1, 2019.

[2] 3. A. H. L and A. A. G. Iman Sharafaldin, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", Proc. 4th Int. Conf. Inf. Syst. Secur. Priv., no. Cic, pp. 108-116, 2018.

[3] 4. V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection", Comput. Networks, vol. 136, pp. 37-50, 2018.

[4] 9. P. Maniriho, Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches, no. April, 2020.

[5] 10. K. M. Sudar, P. Nagaraj, P. Deepalakshmi and P. Chinnasamy, "Analysis of Intruder Detection in Big Data Analytics", 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5, 2021.

[6] 11. K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques", 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5, 2021.

[7] 12. V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea et al., "Optimal Deep Reinforcement Learning for Intrusion Detection in UAVs", CMC-Computers Materials & Continua, vol. 70, no. 2, pp. 2639-2653, 2022.

[8] Ajani, S., Amdani, S.Y. (2022). Obstacle Collision Prediction Model for Path Planning Using Obstacle Trajectory Clustering. In: Sharma, S., Peng, SL., Agrawal, J., Shukla, R.K., Le, DN. (eds) Data, Engineering and Applications. Lecture Notes in Electrical Engineering, vol 907. Springer, Singapore.

[9] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou and A. Derhab, "CyberSecurity attack prediction: a deep learning approach", 13th international conference on security of information and networks, pp. 1-6, 2020, November.

[10] A. G, V. Mohanavel, M. Tamilselvi, G. Ramkumar and R. T. Prabu, "An Intelligent LoRa based Women Protection and Safety Enhancement using Internet of Things," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 43-48, doi: 10.1109/I-SMAC55078.2022.9987425.

[11] S.A. Salloum, M. Alshurideh, A. Elnagar and K. Shaalan, "March. Machine learning and deep learning techniques for cybersecurity: a review", The International Conference on Artificial Intelligence and Computer Vision, pp. 50-57, 2020.

[12] Z. Ahmad, A. Shahid Khan, C. WaiShiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, pp. e4150, 2021.

[13] V. Ramachandran and V Kishorebabu, "A Tri- State Filter for the Removal of Salt and Pepper Noise in Mammogram Images", J Med Syst, vol. 43, no. 40, 2019, [online] Available: https://doi.org/10.1007/s10916-0181133-0.

[14] R. T. Hadke and P. Khobragade, "An approach for class imbalance using oversampling technique", Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 11, pp. 11451-11455, 2015.

[15] M.A. Ferrag, O. Friha, L. Maglaras, H. Janicke and L. Shu, "Federated deep learning for cyber security in the internet of things: Concepts applications and experimental analysis", IEEE Access, vol. 9, pp. 138509-138542, 2021.

[16] J. Zhang, L. Pan, Q.L. Han, C. Chen, S. Wen and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey", IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 3, pp. 377-391, 2021.

[17] D. L. Marino, C. S. Wickramasinghe, C. Rieger and M. Manic, "Data-driven Stochastic Anomaly Detection on Smart-Grid communications using Mixture Poisson Distributions," IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 2019, pp. 5855-5861

[18] R. Sharma, C. A. Chan and C. Leckie, "Evaluation of Centralised vs Distributed Collaborative Intrusion Detection Systems in Multi-Access Edge Computing," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 343-351.

[19] H. Benmoussa, A. A. El Kalam and A. A. Ouahman, "Distributed intrusion detection system based on anticipation and prediction approach," 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France, 2015, pp. 343-348.

[20] Prashant Khobragade, Latesh G. Malik,"A Review on Data Generation for Digital Forensic Investigation using Datamining", IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014.

[21] S. I. Popoola, G. Gui, B. Adebisi, M. Hammoudeh and H. Gacanin, "Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks," 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021, pp. 1-6

[22] Zha, L.; Liao, R.; Liu, J.; Xie, X.; Tian, E.; Cao, J. Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks. IEEE Trans. Cybern. 2021, 52, 13800–13808.

[23] Qu, F.; Tian, E.; Zhao, X. Chance-Constrained H-infinity State Estimation for Recursive Neural Networks Under Deception Attacks and Energy Constraints: The Finite-Horizon Case. IEEE Trans. Neural Netw. Learn. Syst. 2022. 2014

[24] Khetani, V. (2022). Advanced numerical methods for solving partial differential equations in structural engineering. EngiMathica: Journal of Engineering Mathematics and Applications, 1(1).

[25] Rajawat, A. S., Goyal, S. B., Solanki, R. K., Gadekar, A., & Patil, D. (2024). Dark Web Financial Fraud Identification Using Mathematical Models in Healthcare Domain. JOIV: International Journal on Informatics Visualization, 8(1), 107-114.

[26] Nemade, B., Mishra, R., Jangid, P., Dubal, S., Bharadi, V., & Kaul, V. (2023). Improving Rainfall Prediction Accuracy Using an LSTM-Driven Model Enhanced by M-PSO Optimization. Journal of Electrical Systems, 19(3).

[27] Mishra, R., Nemade, B., Shah, K., & Jangid, P. (2023). Improved Inductive Learning Approach-5 (IILA-5) in Distributed System. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 942-953.

[28] Gulhane, M., Kumar, S., & Borkar, P. (2023, November). An Empirical Analysis of Machine Learning Models with Performance Comparison and Insights for Heart Disease Prediction. In 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS) (pp. 374-381). IEEE.

[29] Goyal, Dinesh , Kumar, Anil , Gandhi, Yatin & Khetani, Vinit (2024) Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 703–714, DOI: 10.47974/JDMSC-1921