International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Oct-24)

http://dx.doi.org/10.12785/ijcds/1601116

Enhanced Security Measures in Advanced Wireless Sensor Networks: Multi-Attack Prevention Strategies

M. Arvindhan[1], B.Bharathi Kannan[1], Srinivasan Sriramulu[1], Sunil Kumar[1] and Sudeep Varshney[2]

[1]*School of Computer Science and Engineering, Galgotias University, Greater Noida 201310, Uttar Pradesh, India*
[2]*Department of Computer Science Engineering School of Engineering Technology, Sharda University, Greater Noida 201310, Uttar Pradesh, India*

Received 15 Apr. 2024, Revised 9 Jul. 2024, Accepted 12 Jul. 2024, Published 1 Oct. 2024

Abstract: Distributed denial of service (DDoS) attacks is coordinated attempts to make a system or service unavailable to its intended users by flooding them with traffic or otherwise overloading it with unnecessary requests. Attacks that originate at the application layer of the network are more challenging to detect because they masquerade as legitimate traffic. Networks are protected from distributed denial of service attacks using a disarray-theory-based, six-step strategy that relied on the Cooperative-Based Fuzzy Artificial Immune System (Co-Fais) to determine whether the traffic was malicious. To address the issue of power security, the event acknowledgment method employs the Sequential Probability Ratio Test (SPRT) and the informational character of data. The Destination Oriented Directed Acyclic Graph (DODAG) is an RPL-based alternative to the underlying Routing Protocol for Low Power and Loss Networks that ensures the seamless flow of data from beginning to end in a sensor network that is geographically dispersed and whose communication is disrupted by natural disasters (RPL). QoI-aware RPL could save power by gathering the same information with less data transfer. However, the entertainment industry is rife with blunders due to randomly constructed perceptual frameworks, and the reliability of replicated results is lower than it would be with a more methodical approach. Therefore, it is difficult to keep track of additional component information from the underlying sign while minimizing replication errors. To provide a more precise signal of enjoyment while requiring less storage space, a powerful tension and multiplication process is required. This review employs a modified bat technique to increase the perceptual cross-section and thus get around this obstacle. DDoS attack prevention uses Co-Fais and SPRT methods in wireless sensor networks. The entertainment industry is rife with blunders due to randomly constructed perceptual frameworks, and the reliability of replicated results is lower than with a more methodical approach.

Keywords: QoI-aware RPL, DDoS attacks, Sequential Probability Ratio Test (SPRT), Destination Oriented Directed Acyclic Graph (DODAG), Cooperative-Based Fuzzy Artificial Immune System (Co-Fais)

1. Introduction

A Wireless Sensor Network (WSN) is a decentralized network including numerous sensor nodes that are flexibly interconnected to monitor various physical or environmental parameters, including temperature, sound, pressure, etc. These nodes collaborate to transmit their collected data to a central point via the network. Every individual node has the ability to detect, analyses, and send data. Wireless Sensor Networks (WSNs) are distinguished by their use of wireless communication and their dependence on sensor nodes, whose are commonly powered by batteries and have restricted compute and storage capacities [1]. These networks employ diverse communication protocols specifically developed to preserve energy, which is a vital resource in Wireless Sensor Networks (WSNs). Methods like as data aggregation, which involves combining data from various sensors to reduce the amount of transmissions, and duty cycling, which involves nodes alternating through active and sleep states to conserve energy, are frequently used to prolong the network's lifespan. Furthermore, Wireless Sensor Networks (WSNs) utilize routing strategies such as low energy adaptive clustering hierarchy (LEACH) and power-efficient collection in sensor information systems (PEGASIS) to improve energy efficiency [2]. The purpose of these protocols is to reduce energy usage when transmitting data, which is a difficult task because sensor nodes have a limited battery life. Notwithstanding the progress made in WSN technology, there are still some difficulties that need to be addressed. First and foremost, the issue of energy efficiency remains of utmost importance, as the limited energy reserves of sensor nodes restrict the network's operating lifespan. Furthermore, the security of Wireless Sensor Net-

E-mail address: saroarvindmster@gmail.com, bbharathikannan@gmail.com ramuluvasan@gmail.com, sunildangikc107@gmail.com, sudeep149@gmail.com

works (WSNs) is of utmost importance given the sensitive nature of the data gathered and the possibility of malevolent assaults on these networks. Acquiring information is a crucial field of study. Every tangible aspect, condition, and operation in existence may be explained using physical measurements, and sensors can be employed to gather data on these physical measurements. The technology for acquiring sensor information has progressed from its initial state of singularity to integration and networking, becoming a significant method of gathering information. A wireless sensor network (WSN) is a system consisting of multiple sensors that are spread out in different locations and work together to establish reliable and efficient communication among themselves [3]. To protect the integrity of data and the durability of the network, it is necessary to have strong security measures in place to address difficulties such as data interception, unauthorised access, and node compromise. Moreover, the deployment of WSNs in complex and dynamic systems presents considerable problems in terms of scalability and adaptability. To guarantee that Wireless Sensor Networks (WSNs) can handle a significant number of sensor nodes and adjust to varying environmental conditions while maintaining optimal performance and energy efficiency, it is necessary to employ advanced network design and management methodologies. Hence, it is imperative to prioritise the optimisation of wireless communication transmission and the attainment of robust security performance in WSN research [4]–[7]. As a result of these developments, the dependability and safety of wireless sensor networks, however, have grown more susceptible to a variety of threats. Advanced wireless sensor networks are particularly vulnerable to assaults, including eavesdropping, tampering, and unauthorized access, all of which can jeopardize the data's integrity and confidentiality while also threatening the networks' entire operation and performance. Research on state-of-the-art networking techniques emphasising preventing multiple attacks has grown in importance as a means to meet these problems.

The research objectives of our research paper as following:

- Enhancing Energy Efficiency in WSNs: Develop advanced protocols and strategies, such as data aggregation and duty cycling, to extend the operational lifespan of sensor nodes in Wireless Sensor Networks (WSNs) while maintaining optimal performance.
- Strengthening Security Measures: Implement robust security protocols to protect data integrity and network resilience against various threats, including unauthorized access and malicious attacks, ensuring secure transmission and storage of sensitive information.
- Optimizing Network Scalability and Adaptability: Explore innovative network design methodologies and management techniques to enhance the scalability and adaptability of WSNs, enabling efficient handling of diverse environmental conditions and large-scale deployments.
- Integration of Deep Reinforcement Learning (DRL): Investigate the application of Deep Reinforcement Learning (DRL) techniques in WSNs to optimize decision-making processes and resource management, leveraging the capabilities of DRL to overcome challenges posed by limited node resources.

The healthcare, autonomous vehicles, and smart grid administration industries have been greatly influenced by the rapid advancement of deep learning and reinforcement learning methodologies in the past few decades. These technological improvements have resulted in the development of deep reinforcement learning (DRL), which is a very effective tool that brings together the capacity for representation of deep learning with the capacity for decision-making of reinforcement learning. Deep Reinforcement Learning (DRL) is very effective in situations where obtaining the best course of action involves comprehending intricate data and making a series of decisions in a certain order. This makes DRL especially well-suited for use in Wireless Sensor Networks (WSNs). Due to the limited resources (battery life, memory, and attention) available at individual nodes within LLNs, inter-node connections can be difficult to establish and maintain. Wireless sensor networks (WSNs) are a type of LLN in which data is gathered from sensors and transmitted to a central hub, where it can be processed [8]. WSN centres are crucial in remote assortment frameworks due to their compact size, low energy consumption, and user-friendliness for executives in different locations. The transmission of data uses up a lot of power in sensor nodes [9]. However, the huge amount of data in WSNs severely limits the utility of the central node. One motivation behind this innovation was the need to lessen the energy footprint of distributed sensor networks employing RPL for event detection.

This paper's primary contributions can be briefly summarized as follows:

1) We proposed a RPL instance framework for determining the selected slave node for interfacing with a malicious group. This framework provides a structured approach for identifying and selecting appropriate slave nodes within a RPL network to effectively counteract malicious activities.
2) We conducted experimental verification to demonstrate the effectiveness and superiority of our proposed framework in countering attacks in Wireless Sensor Networks (WSNs). Through empirical testing and analysis, we validated the efficacy of our approach in enhancing the security and resilience of WSNs against various types of attacks.
3) We integrated the outcomes of our framework with the Bat algorithm, utilizing its working principles and applications. By incorporating the Bat algorithm into our proposed RPL instance framework, we enhance the adaptive and dynamic nature of the

system, allowing it to effectively respond to changing network conditions and evolving security threats.

The rest of this paper is organized as follows. In Section 2, we have discussed the background work. In Section 3, we have discussed the related work. The proposed framework and its key components are discussed in Section 4. In Section 5, we have discussed the experimental analysis and comparison with baseline and state-of-the-art techniques. Finally, Section 6 discussed about the results obtained and Finally in Section 7 highlights conclusion and future research.

2. Background

Unlike collection-based steering conventions, QoI-conscious directing conventions. In these systems, each hub picks the next leap alongside the organization as the encompassing hub with the most anticipated data addition, and when the combined data exceeds a particular limit, it is conveyed to the root. In WSNs, IQAR [10]–[12] utilizes a tree-based methodology, albeit the blended community at the lower part of the tree uses more energy.

A. RPL and DODAG Construction

The DODAG Information Object (DIO) is useful for monitoring an RPL Instance, gathering information about its arrangement's bounds, selecting a DODAG close relative locate, and keeping tabs on the DODAG itself from a central location. When a new neighbour joins the DODAG, it is directed to the DODAG root, which becomes the center's parent in the DODAG. Focuses A receives a DIO message from the DODAG root containing DODAG data, then joins the DODAG and sends a DAO message to the root containing prefix data. Then, focal point A sends focal point B a DIO message; focal point B retrieves the DODAG data within focal point A's transmission scope, joins the DODAG, and replies with a DAO significance toward focal point A.

The DODAG Information Object (DIO) can be used by a hub to observe an RPL Instance and gather facts about its structure [13]. Donoho et al. proposed a method for quickly calculating a vector and then resetting it to the Euclidean accuracy range. Fang et al. constructed the sub-Gaussian appointment inadequate discernment grid. Duarte et aleigen values corruption method was used to improve the sporadic Gaussian detection system. Transforming the Gram cross section into a unit structure was a task undertaken by Lan et al. Decentralized nature and lack of fixed infrastructure make MANETs vulnerable. Impact on legitimate traffic minimized during DDoS attack prevention. High density and limited communication range of sensor nodes Lack of centralized monitoring and overprotective requirements.

B. Types of Security and Attacks

Due to association defects, poor actual assurance, dynamic topological changes, and availability anomalies, security in remote portable organizations is challenging to supply. Because the trust connection between communication hubs varies continually due to topological changes [2], a security technique based on static type design will be worthless.

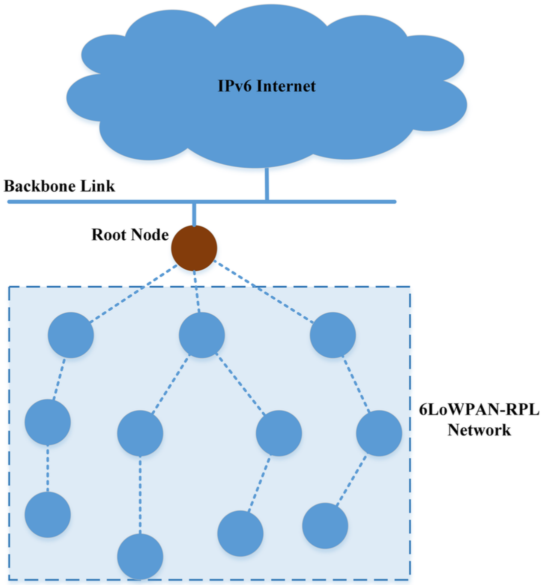

Figure 1. 6LoWPAN RPL-based IoT Network

Security isn't only an issue for the organization's members. The communication links should not be exposed to any kind of assault while the information is being sent. A programmer may focus on a communication channel, get the mysterious keys, decode them, and infiltrate the company with fake information. Organizational security, such as computer security and e-mail encryption, is critical. To establish a safe organization, as demonstrated in [3] a few considerations must be taken.

Internet attacks: It's feasible to classify them into various gatherings. Individual information and framework subtleties are acquired utilizing phishing and tuning in assaults. Worms, infections, and Trojan ponies are instances of assaults that might make a framework's standard working upset. A disavowal of administration assault is one in which the system's assets are depleted to the point that it is delivered ineffectually.

Eavesdropping: At the point when an unapproved individual records a conversation, this is known as snooping. Sneaking around might be inert or dynamic; in the previous, the interloper simply pays attention to the channel, while in the last option, the intruder pays attention to the transmission first and afterward adds clandestineness material. As a result, information might become muddled or information that was recently covered might be eradicated. The two worms and diseases can self-repeat. Conversely, the first needn't bother with a report to repeat and spread across the structure [4]–[6]. The two most regular sorts of worms are network item worms and mass-mailing worms. A worm that knows about the association chooses an objective and taints it with a Trojan or other programming. Email is a strategy for polluting the objective in mass-mailing worms.

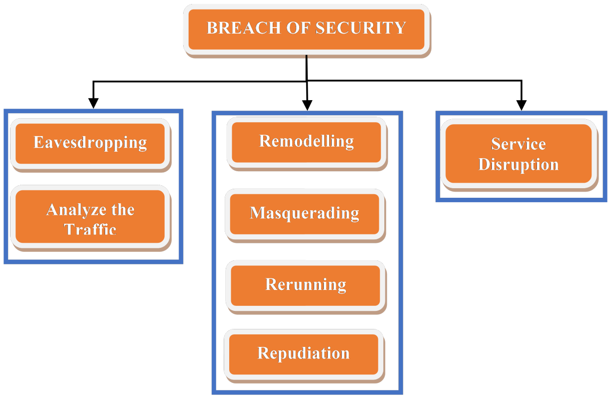

Figure 2. Attack Types

- **Confidentiality:** The information on the network is kept confidential.
- **Network communication:** Only authorized users have access to the network.
- **Integrity:** Guarantees that information isn't altered on the way and shows up at its objective in its unique condition.
- **Authentication:** This assures that the organization's clientele is who they claim to be access control unit.
- **No repudiation:** Assures that the user does not deny using the network.

Trojan horses Viruses: Debases records and spreads all through the construction [4] by replication. Diversions appear to be faithful to the system, yet they have a secret plan. They much of the time have a payload, as an illness. [4]. Phishing is a technique for acquiring delicate data from an individual, a gathering, or an association [5]. Clients are fooled into giving over close-to-home data, monetary data, Visa data, and other delicate data utilizing phishing attacks.
IP Spoofing Attacks: The area of an upheld PC is cloned and used to mimic a guaranteed center point to gain admittance to different PCs on the organization in this sort of assault. Countermeasures and recognition are trying since the foe's character is concealed in various ways. Indeed, even with current association safety efforts, IP ridiculing attacks are hard to stay away from [4].
Denial of Service (DoS): A digital assault against a firm fully intent on keeping it from working appropriately? Countless dangerous information packs are infused into the association in this sort of attack. They are gathered by network center points and appropriated to enveloping centers. In all actuality, it's a multi-pronged assault [6]–[8]. Many sorts of DoS attacks, like an accident, changing, and staying, happen at various degrees of far-off sensor associations.

3. Related Works

To research, the impact of the remark framework on the arrangement of rules, five diverse comment networks and a set of rules-improved proclamation grids are utilized to reproduce the sign. Nearer to the end, signal reproduction is finished.
In [8], a game idea approach dependent on UDSR (Utility-based unique inventory directing), which is created from DSR (Dynamic Source Routing), be use seeing that a got steering convention, and an eye list is utilized to track down restricting hubs The utility expense is used to pick the most helpful way, while notoriety and participation are utilized to evaluate hub misconduct. Utilizing this maverick hub no longer damages the primary organization. Every specialist in a multi-specialist immunological gadget has its arrangement of objectives and obligations.
In [nine], The idea of a public closeout is applied to the creation of conflicting nodes. To identify a malicious hub inside the network, Purpose employs a broken clock: if the timer expires before a package reaches the escape zone, a message with a broken heading is sent off the base hub, and the remaining hubs in the network are taken off the watch list. Due to the widespread practise of hubs ignoring negative acknowledgment hubs, the overall scope of packages lost in SAR remains constant [14], [15]. A CH is chosen by considering the total amount of unused energy in the group's hubs in addition to the verbal trade cost between bunches, which is a function of both the group's thickness and the hubs' degrees. Assuming a hub is found locally, a convention is made to perceive the hub that takes part in a decent day flood attack. Humaira Ashraf et al. propose an innovative defense algorithm to mitigate Black Hole Attacks (BHA) in Wireless Sensor Networks, significantly enhancing network longevity by 43.3% over previous methods. Utilizing NS2 and Simulink for extensive simulations, their research evaluates network throughput and Packet Delivery Ratio (PDR) to safeguard IoT networks against BHA. This approach offers a robust solution to a critical security challenge, ensuring more reliable and efficient network performance.

The list of survey made on the above section explains proposed approach offered efficient identification and reliable pinpointing of malevolent intrusions. The optimized LSTM surpasses the traditional LSTM in terms of accuracy in detecting attacks. A centralized technique enhances the rate at which malicious nodes are detected. Improves characteristics such as throughput and decreases average latency. WSNs face significant identification challenges in practical applications. Machine learning is used to develop a smart ID strategy in WSNs. The most recent studies have concentrated on finding ways to combat distributed denial of service (DDoS) assaults in WSNs, both centrally and decentrally. Strong security and effective power management are achieved through the use of these techniques, which

TABLE I. Comparison of Wireless Network Security approach and methods used

Author & Year	Insights	Methods Used	Merits	Limitations
Humaira Ashraf et.al.[[16]]	MABPD utilizes mobile agents, authentication, and trust values to detect Black Hole Attacks in Wireless Sensor Networks, significantly improving energy consumption, packet delivery rate, and network lifetime.	Mobile agents with authentication of nodes.Trust values to detect black hole nodes	Packet delivery rate increased by 19.51%. Energy consumption reduced by 53.3%, network life increased by 43.3%	Existing schemes reduce energy but fail to decrease packet drop ratio. Detection algorithm increases energy consumption, enhancing network lifetime.
Gebrekiros GG et.al.[[17]]	An optimised multilayer perceptron artificial neural network localises and detects numerous threats in wireless sensor networks, improving security.	Using optimised multilayer perceptron artificial neural networks for cybersecurity localization	Accurately detected DoS attacks. Improved localization precision and accuracy above state-of-the-art solutions.	Detecting WSN DoS attacks using machine learning.
Ponnuswami V et.al. [[18]]	The research proposes techniques to identify and prevent DOS assaults in IoT-based Wireless Sensor Networks employing numerous base stations, improving security, energy efficiency, and network lifespan.	Multiple base stations and a key are used for detecting DOS attacks.	Detection and prevention of DOS attacks in IoT-based WSN.	Protocols are used to reduce above them, boost packet their delivery, and extend the lifespan of the network.
Iftikhar Hussain et.al.[[19]]	WSNs' soft determination and preventative method prevents collision and burnout attacks, improving node lifetime, network performance, throughput, and delay.	Soft decision mechanism for collision and exhaustion attacks detection.	Increased node lifetime and network performance with reduced energy consumption.	Limited access to medium, paralyzing communication. Nodes desperate for medium access, affecting network services.
Pankaj.R et.al. [[20]]	Convolutional Neural Networks for sensor networks that are wireless are used to create an intrusion detection system that prevents multiple hacking attempts with 97% accuracy, outperforming current technologies.	Deep packet inspection based on convolutional neural network	Intrusion prevention system using CNN for WSN	Intrusion detection and prevention using deep learning model
Charu Sharma et.al. [[21]]	DH-SAM, which uses AOMDV for multiple paths of routing, can identify avoid security across multiple attacks at once.	Diffie-Hellman key exchange for secure communication. AOMDV multipath routing protocol for data transmission	Multipath routing for availability and consistency of data transmission	Single path routing: link failure, compromised node data security. Diffie-Hellman key exchange: vulnerable to MITM attacks without authentication.

combine cryptographic methods with traffic monitoring and network architectural design. Unfortunately, particular solutions for managing power consumption in wireless sensor networks are not adequately covered in the search results Tab.1 .

Existing research demonstrates advancements in threat detection accuracy, energy efficiency improvements, and enhanced network performance. Technologies like MLP-ANN and CNNs offer robust solutions for real-time threat detection, while multilayered security protocols and multipath routing strategies improve overall network resilience. Common weaknesses include increased computational overhead in detection algorithms, potential vulnerabilities in protocol implementations, and challenges in scalability for large-scale deployments. Some methods may also struggle with real-time responsiveness or require significant computational resources.

A. *Existing Challenges and Gaps*

Deploying and operating WSNs provide significant problems, particularly in achieving a balance between energy efficiency and robust security measures. Conventional methods frequently address these problems separately, resulting in network performance that is less than ideal. Some of the main difficulties are as follows:

1) Enhancing the effectiveness of energy utilization. Due to the limited power resources of sensor nodes, it is crucial to find ways to prolong the network's lifespan while ensuring that it continues to function effectively.
2) Security. Wireless Sensor Networks (WSNs) are vulnerable to various security risks due to their open communication nature, including data breaches and node tampering. Therefore, it is crucial to implement comprehensive security measures to protect WSNs.
3) Mobility. Adaptable techniques are necessary due to dynamic network conditions and developing threat landscapes, which cannot be addressed by standard static methods.

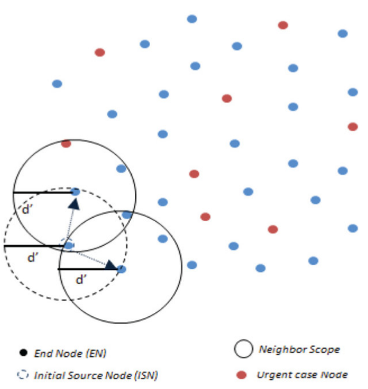

Figure 3. Structure of neighborhood findings in suggested scenarios

4. Proposed Work

DDoS attacks, or distributed denial of service attacks, are a more sophisticated form of DOS attacks in which a malicious command and control node selects a slave and the slaves flood the legitimate command and control node with malicious groups that interfere with network execution. When a DDOS attack occurs and all of the association's data centres begin sharing data, the throughput of the entire network drops below a certain threshold, initiating a vicious cycle of harmful perceived evidence from a subset of the network's centres.

Centers that send data packages across the border during the malignant centre time window are referred to as toxic centre points, and the watchman canine procedure is used to determine whether or not these centres are sending data bundles or control groups. In the context of data transmission, the nodes in the centre are referred to as slave nodes or slave nodes. The communicating hub is labelled the malignant centre of the network when slave nodes receive command packets from it.

A strategy framework known as Disarray Theory might help you acquire an advantage in the market by capitalizing on disruption and unpredictability. Step one is to analyze the present condition of the market. Step two is to identify any weaknesses in opponents or inefficiencies in the marketplace. Step three is to develop unconventional tactics that can be challenging to foresee. Step four is to implement these approaches in order to disrupt the market. Step five is monitoring their effect to determine how effective they were. Finally, step six is to continually modify tactics to keep up the benefits. This strategy seeks to gain a lasting edge over rivals by disrupting their operations and seizing opportunities in the market through quick thinking and innovation fig. 4.

Our framework draws parallels with Disarray Theory, focusing on market disruption and unpredictability. This involves analyzing market conditions, identifying competitors' weaknesses, and exploiting market inefficiencies. We develop innovative strategies that are challenging to anticipate, implement them to disrupt adversaries, and continuously adapt tactics based on their impact. This approach aims to gain a sustainable competitive advantage by leveraging disruption and seizing market opportunities effectively. This methodological approach integrates insights from network security and strategic management theories, providing a comprehensive strategy for combating DDoS attacks while aligning with broader market disruption strategies.

To model the impact of a Disarray Theory-based strategy, we can use a system of differential equations to represent the dynamic interactions between the company (C) and its competitors.

$$\frac{dC}{dt} = \alpha C\left(1-\frac{C}{K}\right) - \beta CR \tag{1}$$

$$\frac{dR}{dt} = \gamma R\left(1-\frac{R}{K}\right) - \delta CR \tag{2}$$

Where:
α and γ are the growth rates of the company and competitors, respectively

- K is the carrying capacity of the market.
- β and δ are the interaction coefficients representing the impact of competition.

A. Several different RPL Instances may be found on a network that uses the RPL Protocol

A DODAG in each RPL Instance framework has the same RPL Instance ID, and each RPL Instance is made up of one or more DODAGs that are all unique. As a consequence, each RPL Instance ID may be used to identify a particular RPL Instance inside the framework, and each RPL Instance is composed of a set of unique arbitrary whole numbers. All DODAGs in the same RPL Instance utilize the same equivalent of [9], [16] at the end of the day. As shown in Figure 4, different RPL Instance frameworks have distinct arbitrary Numbers.

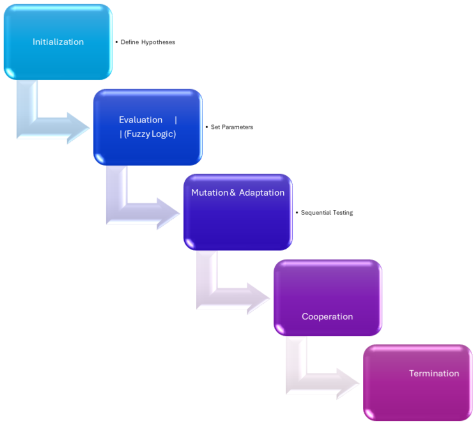

Figure 4. The RPL protocol's relationships between numerous parts

1) Bloom Filters in Network Security Applications

We'll take a gander at network safety efforts that utilization BFs and their unique structures, either straightforwardly or in a roundabout way, in this part. These segments demonstrate whether the Bloom directs used in every security field are embedded in end-contraptions (ED), transitional devices (ID), or maybe in-pack (IP), where the Bloom channel is kept inside the bundle across the association [17], [20].

B. Bat Algorithm Working and its Application

Xin-She Yang fostered the Bat Algorithm in 2010 to utilize bat echolocation. The bats use sonar resonations to find limits using sound pulses that have been modified to another rehash. On a size of 0 to 1, with 0 showing no surge and 1 addressing the most extreme, this heartbeat rate might be registered:

Algorithm 1 DODAG with RPL Algorithm

```
 1: Broadcast_DIS()
 2: while DIOs not received do
 3:     Continue broadcasting DIS
 4: end while
 5: for each received DIO do
 6:     if C_ID(mobile_node) $\leq$ C_ID(neighbor) then
 7:         Set neighbor with greatest quality as best parent
 8:     end if
 9: end for
10: while True do
11:     if C_ID(neighbor) changes then
12:         Reject DIO and broadcast DIOs
13:     else
14:         Wait until timer runs out
15:     end if
16:     if Data forwarding to parent node not feasible then
17:         Go to step 5
18:     end if
19: end while
20: Send_data_to_highest_corona_level_node()
21: Inform_child_nodes_to_cease_transmission()
22: while True do
23:     Continue_sending_data_packets_via_neighbors()
24:     if new candidate found then
25:         Break
26:     end if
27: end while
```

Algorithm 2 Bloom Filter Algorithm

```
for i = 1 to l do
    Select hash capacity Hi from the list H1...Hl
    Store S in Bloom filter BFS using hash function Hi
    if x is in BFS then
        Output 1
        Return
    end if
end for
```

1) In a surprising way, all bats use echolocation to assess separates and foresee the error between their prey and establishment tangles.
2) Bats y aimlessly while looking for food, with a speed of vi at xi, a reasonable repeat of fmin, a variable recurrence, and an A0 tumult. The bats might change their pulse radiation rates (beat surge r ¿ [0; 1]), which is subject to the objective and its district, autonomously.
3) Regardless of whether or then again on the off chance that the disturbance vacillates, we ought to accept it does as such between the colossal (positive) A0 and the base steady worth Amin.

Algorithm 3 Bat Algorithm

```
Initialize objective function f(x)
Initialize parameters
$n \leftarrow number\_of\_bats$
$Q\_min \leftarrow$ minimum frequency of pulse
$Q\_max \leftarrow$ maximum frequency of pulse
$A\_min \leftarrow$ minimum loudness
$A\_max \leftarrow$ maximum loudness
$t \leftarrow 0$
$Tmax \leftarrow$ maximum number of iterations
Generate initial population of bats
for i = 1 to n do
    Initialize position xi and velocity vi
end for
while $t < Tmax$ do
    for each bat i do
        Generate random frequency Qi within [Q_min, Q_max]
        Generate random pulse rate ri and loudness Ai within [A_min, A_max]
        Update bat's position and velocity
        $xi\_new \leftarrow xi + vi$
        $vi\_new = vi + (xi\_best - xi) * Qi$
        End Update
        if rand(0,1) ¡ Ai and f(xi_new) ¡ f(xi) then
            Accept new solution: xi = xi_new
            Update loudness and pulse rate:
            Ai = alpha * Ai, ri = ri * (1 - exp(-gamma * t))
        end if
    end for
    Update iteration count: t = t + 1
end while
Find the best solution among all bats
Output the best solution
```

5. Method

A. Hierarchical Trust Management Model for Wireless Communication Networks

Notwithstanding the way that it is a far-off correspondence network with differing levels of trust, the chiefs model is presented recorded as a hard copy [18], [22]–[25]. The association model, then again, neglects the base station's dynamic ability (BS). This present model's bundle head is genuinely fixed. The capacity of an association to stay working however long plausible while devouring as little energy as conceivable is alluded to as energy adequacy.

1) By changing a sensor from functional to "rest" mode, the energy utilization of the sensor might be limited. This may be improved by bringing down the number of groups sent between center points. WSN is isolated into different gatherings all through this methodology.
2) It reduces the number of calculations the sensor center does (SN).
3) Use the data combination way to deal with managing diminished WSN energy use.
4) The aggregator gathers information from a few center points, decides the complete limits, and illuminates the association facilitator regarding the discoveries. The complete expense of information transmission is extensively diminished when contrasted with the situation preceding the aggregator [19]–[21].

The information related to center point N is added to the reliable center information assortment assuming that center point N finishes the assessment. All center points in a similar gathering will from there on receive messages pertinent to a center point N. Assuming center point p finds uniqueness in center point q, it will establish a connection with CH, and CH will settle on a choice on center q.

1) Module for gathering data

Neighbors are two hubs that are within a similar transmission and collecting a range of distance. A certain hub may be able to acquire direct information about information bundles due to the transmission characteristics of the distant media. Observing all of the hubs' edges in the MAC layer, and recording the information parcel's broadcast information, allows one to learn about the surrounding area's behavior. A condition should be specified if the WSN is bunch-based. The most significant need is that the hubs be located in an area with a similar population.

2) Module for calculating trust levels

We've provided a formula for determining the amount of trust.

$$A_{pq} = \frac{i_1 X_{pq} - i_2 Y_{pq}}{i_3 X_{pq} - i_4 Y_{pq}} \tag{3}$$

Node p's trust value toward node q is expressed as A_{pq}. The number of successful q events observed by p is given by Xpq, while the number of unsuccessful q proceedings is given by Ypq. In comparison to the weight/importance of unsuccessful occurrences, i_1, i_2, i_3, and i_4 represent the weight/importance of successful events. For each network event, the trustworthiness value determination is computed. The trust ratings connected to these activities are then compounded by the weight factor X to demonstrate their significance in the sanctuary point. Determine the node's total dependability by appending these in someone else's company.

The formula for the precise computation is exposed in procedure (or) formula (2). We may also acquire the amount of constancy.

$$G_{pq} = \sum_{i=1}^{m} x_i * Apq' \tag{4}$$

$$L_e = \frac{x_i * E + x_2 * d * G_{pq}}{x_3 * L} \tag{5}$$

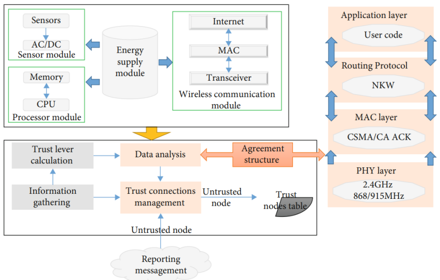

Figure 5. The trust management systems architecture

E denotes the remaining energy level among them. The node's mobility level is indicated by the letter L, while the distance from the base station is indicated by the letter d. The stability level is denoted by the letter L_e.

3) Module for managing trusted connections.

To establish the confidence level, the module uses the following algorithm:

1) Cluster Head obtains the parameter beginning the analyzer
2) Cluster Head requirements Ea and Ga from sensor node a
3) Cluster Head calculates Gb using formula (2) based on the parameters received
4) Cluster Head compare the morals: continue the method if Ga = Gb; otherwise, the inaccurate value of a becomes untrustworthy
5) Cluster Head does a comparison between E and the quantity of packet transmitted.
6) The follow requirements must be met.

$$
\begin{aligned}
E &= max(0, E_a),\\
E &= min(0, E_a),\\
E &= avg(0, E_a),\\
T_p &= max(min(0, E_a)),\\
T_p &= min(min(0, E_a)),\\
T_p &= avg(min(0, E_a)),
\end{aligned} \tag{6}
$$

7) If these requirements can be maintained, then an is believable; otherwise, the sort of data packet delivered must be examined.
8) The Cluster Head (CH) is responsible for getting initial settings and requesting certain metrics (Ea and Ga) from a sensor node as part of the process that is used to determine the level of trust in sensor networks. Following that, the CH computes a derived metric, which is denoted by Gb, and compares it with Ga. If the two metrics are identical, the procedure proceeds. In addition, the CH examines the number of packets that have been delivered by the sensor node in conjunction with a parameter E and determines whether or not specific requirements, such as threshold values, have been satisfied. In the event that all of the prerequisites are met, the sensor node is regarded as trustworthy; otherwise, the data packets require additional scrutiny. This strategy guarantees that the data that is included within the network is reliable.

6. Results and Discussions

A reliable smart grid requires layered protection, incorporating a cybersecurity architecture that limits unforeseen interruptions (attacks) and flexible energy grid applications capable of maintaining functionality throughout the duration of an attack. We offered an activity in which we arrange to give a summary of the smart grid process, together with cyber security infrastructure and energy grid system station controls, as well as the quality and amount of energy grid delivered to users at that period.

Ensuring the reliability and security of a smart grid necessitates a multifaceted approach, incorporating robust cybersecurity measures and adaptable energy grid applications capable of maintaining functionality throughout varying attack durations. Our study has demonstrated the effectiveness of integrating comprehensive cybersecurity architecture, including proactive threat detection and response mechanisms, to mitigate potential disruptions and ensure continuous grid operation. Moreover, the integration of sophisticated energy grid system controls has enabled real-time monitoring and management of energy distribution, optimizing both the quality and quantity of energy delivered to end-users. By enhancing grid resilience and responsiveness, our approach not only safeguards against cyber threats but also enhances overall grid efficiency and customer satisfaction.

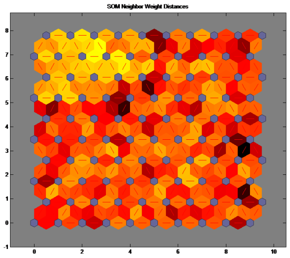

Figure 6. Network Weight Area Analysis

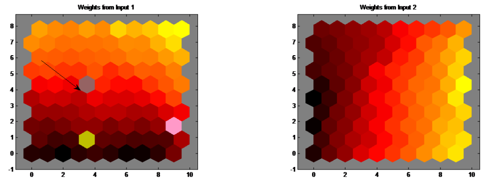

Figure 7. Network Weight 1 and 2 Area Analysis

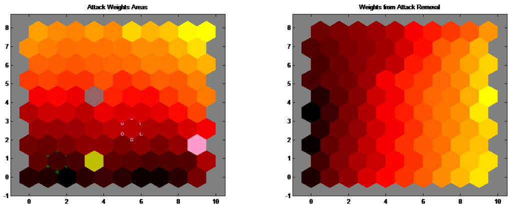

Figure 8. Network Attack Weight and Removal Area Analysis

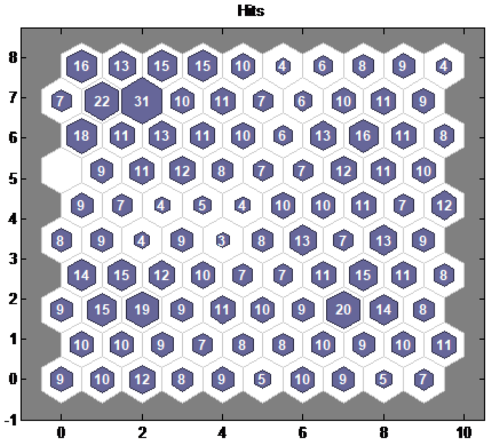

Figure 9. Network Attacks Hits

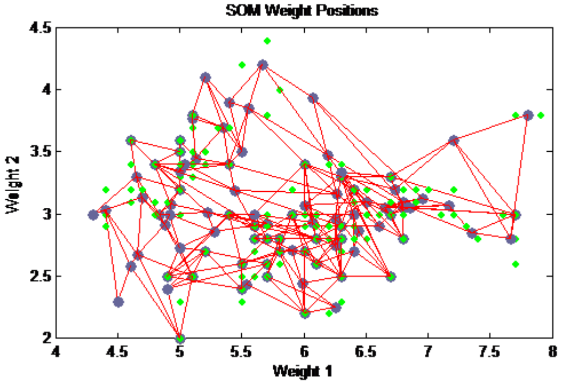

Figure 10. Enter Caption

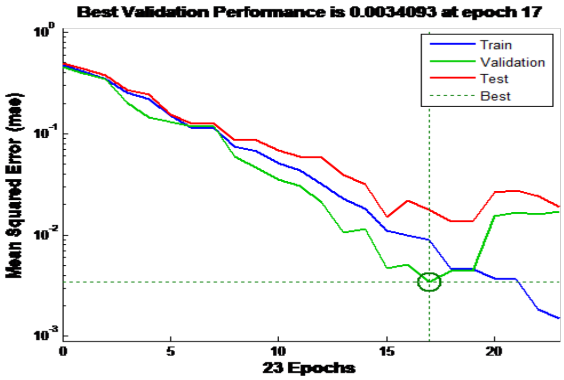

Figure 11. IDS Cluster Nodes Train, Test and Validation Model

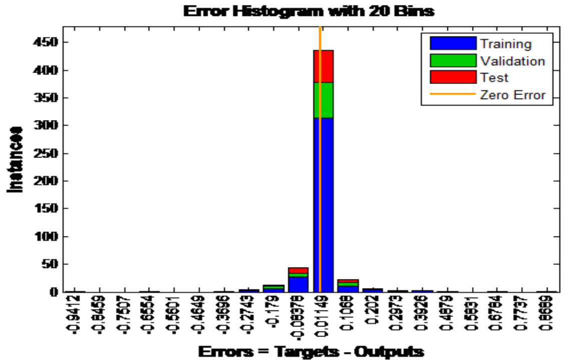

Figure 12. Error Histogram

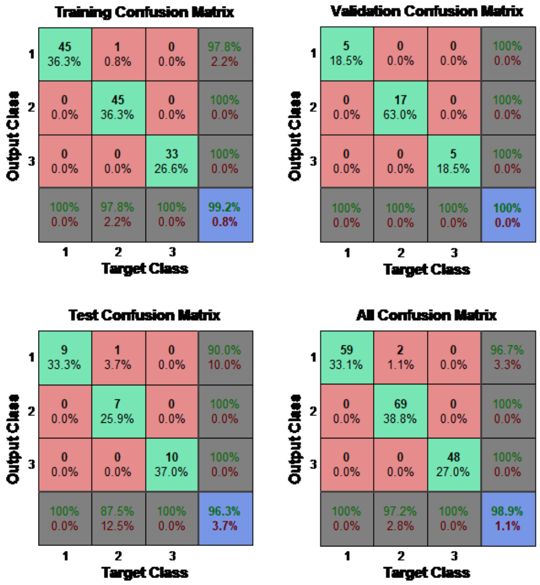

Figure 13. Confusion Matrix

7. Conclusion and Future Work

In conclusion, the concept of data acquired by the sensor is disentangled, the least expensive path for data mix is planned, and steps are taken to reduce additional DODAG links caused by communication failures between the DIO and its receiver through the national list and the DIO's closest relative, in that order. The distinction between DDoS attacks and legitimate traffic is achieved by utilizing controlled and independent fake neural associations. For the best outcomes in a number of real-world rush-hour gridlock situations brought on by DDoS attacks, we used the coefficient from the fluffy model. Using the most recent datasets, our artificial neural networks successfully distinguished between DDoS attacks with a success rate of over 95% gained through the application of two distinct learning methodologies. IoT creation and installation are highly influenced by WSN. The variety of uses of WSN-IoT are growing, and people are increasingly relying upon them. Fully understanding the IoT connection is crucial for improving wireless sensor network reliability and advancing cutting-edge information network technologies in real applications and WSN and optimize technical forms. A few enhancements are suggested on the basis of the electrical power economy and safety aspects of networks of wireless sensors. While WSN innovation in technology faces challenges, its ground-breaking research will significantly impact IoT and advertise the future growth of technological innovations. Efficient attack detection using DODAG for securing wireless sensor networks. Achieved high accuracy rates of 97.21% and 96.86% in real-time datasets. Any how Limited resources and energy of WSN nodes.

In addressing the challenges of securing wireless sensor networks (WSN), our research has focused on distinguishing between DDoS attacks and legitimate traffic using innovative neural network models, achieving over 95% accuracy. Future enhancements could further optimize energy efficiency and network safety, crucial for the widespread adoption of WSN-IoT applications. Addressing these challenges will advance both the reliability of WSN technologies and the broader landscape of IoT, fostering future innovations in network security and management. Inefficient computation due to restricted resources. The future work can be carried out on Difficulty in properly identifying untrusted routing node activities. Lack of effective ways to avoid malicious node attacks.

References

[1] M. E. Haque and U. Baroudi, "Ambient self-powered cluster-based wireless sensor networks for industry 4.0 applications," *Soft Computing*, vol. 25, no. 3, pp. 1859–1884, 2021.

[2] A. Rajput and V. B. Kumaravelu, "Fcm clustering and fls based ch selection to enhance sustainability of wireless sensor networks for environmental monitoring applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1139–1159, 2021.

[3] X. Fu, G. Fortino, P. Pace, G. Aloi, and W. Li, "Environment-fusion multipath routing protocol for wireless sensor networks," *Information Fusion*, vol. 53, pp. 4–19, 2020.

[4] V. Vijayalakshmi and A. Senthilkumar, "Uscdrp: unequal secure cluster-based distributed routing protocol for wireless sensor networks," *The Journal of Supercomputing*, vol. 76, pp. 989–1004, 2020.

[5] S. Kumar, A. Pandey, and S. Varshney, "Exploring the impact of deep learning models on lane detection through semantic segmentation," *SN Computer Science*, vol. 5, no. 1, p. 139, 2024.

[6] S. Kumar, M. Jailia, and S. Varshney, "Improved yolov4 approach: a real time occluded vehicle detection," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 489–497, 2022.

[7] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for dos attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, p. 17, 2023.

[8] J. Bhola, S. Soni, and G. K. Cheema, "Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1281–1288, 2020.

[9] K. A. Darabkh, M. Z. El-Yabroudi, and A. H. El-Mousa, "Bpa-crp: A balanced power-aware clustering and routing protocol for wireless sensor networks," *Ad Hoc Networks*, vol. 82, pp. 155–171, 2019.

[10] P. Majumdar, D. Bhattacharya, S. Mitra, and B. Bhushan, "Application of green iot in agriculture 4.0 and beyond: Requirements, challenges and research trends in the era of 5g, lpwans and internet of uav things," *Wireless Personal Communications*, vol. 131, no. 3, pp. 1767–1816, 2023.

[11] S. Kumar, M. Jailia, and S. Varshney, "An efficient approach for highway lane detection based on the hough transform and kalman filter," *Innovative infrastructure solutions*, vol. 7, no. 5, p. 290, 2022.

[12] S. Kumar, M. Jailia, S. Varshney, N. Pathak, S. Urooj, and N. A. Elmunim, "Robust vehicle detection based on improved you look only once." *Computers, Materials & Continua*, vol. 74, no. 2, 2023.

[13] M. Zhumayeva, K. Dautov, M. Hashmi, and G. Nauryzbayev, "Wireless energy and information transfer in wban: A comprehensive state-of-the-art review," *Alexandria Engineering Journal*, vol. 85, pp. 261–285, 2023.

[14] J. Mu, X. Yi, X. Liu, and L. Han, "An efficient and reliable directed diffusion routing protocol in wireless body area networks," *IEEE Access*, vol. 7, pp. 58 883–58 892, 2019.

[15] S. Kumar, A. K. Upadhyay, P. Dubey, and S. Varshney, "Comparative analysis for edge detection techniques," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 2021, pp. 675–681.

[16] H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Jhanjhi, and M. Humayun, "Mabpd: Mobile agent-based prevention and black hole attack detection in wireless sensor networks," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*. IEEE, 2023, pp. 1–11.

[17] G. G. Gebremariam, J. Panda, S. Indu *et al.*, "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network," *Wireless Communications and Mobile Computing*, vol. 2023, 2023.

[18] P. Vinayagam, P. C. Kumar, P. V. Teja, and P. Maruthi, "Detecting and preventing of dos attacks in an iot based wireless sensor

network," in *2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*. IEEE, 2023, pp. 1–7.

[19] I. Hussain, S. Zahra, A. Hussain, H. D. Bedru, S. Haider, and D. Gumzhacheva, "Intruder attacks on wireless sensor networks: a soft decision and prevention mechanism," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, 2019.

[20] P. R. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 2, p. 504, 2022.

[21] C. Sharma and R. Vaid, "A novel sybil attack detection and prevention mechanism for wireless sensor networks," in *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*. IEEE, 2021, pp. 340–345.

[22] D. W. Wajgi and J. V. Tembhurne, "Localization in wireless sensor networks and wireless multimedia sensor networks using clustering techniques," *Multimedia Tools and Applications*, vol. 83, no. 3, pp. 6829–6879, 2024.

[23] J. Zhang and R. Yan, "Centralized energy-efficient clustering routing protocol for mobile nodes in wireless sensor networks," *IEEE Communications Letters*, vol. 23, no. 7, pp. 1215–1218, 2019.

[24] X. Xiao and R. Zhang, "A danger theory inspired protection approach for hierarchical wireless sensor networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 5, pp. 2732–2753, 2019.

[25] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *Ieee Access*, vol. 6, pp. 7234–7243, 2017.

M.Arvindhan M.Arvindhan is currently working as Assistant Professor in the School of Computer Science and Engineering. he has a total experience of more than 13 years of teaching. He has been associated with Galgotias University since 2017. he is a firm believer in productivity and efficiency at work. he Exhibits an honest work ethic and the ability to excel in a fast-paced, time-sensitive environment. Being a passionate teacher, He believes that teaching is not merely restricted to making the students understand the underlying concepts of a course but also to developing critical thinking and evaluating alternate approaches for problem-solving. He always puts his efforts toward the overall development of his students. He has convened/organized more than 40 co-curricular/Extracurricular events for the benefit of students in the past 5 years.

B.Bharathi Kannan B. Bharathi Kannan is a Research Scholar in the School of Computer Science and Engineering at Galgotias University (GU), Greater Noida, Uttar Pradesh, India. He has completed his B.Tech and M.Tech from reputed institutions. His research interests are primarily focused on Wireless Sensor Networks, Cloud Computing, and the Internet of Things (IoT). B. Bharathi Kannan is actively involved in cutting-edge research projects, contributing to the development of innovative technologies in these areas. His work aims to enhance the efficiency and security of wireless communication systems and to advance the integration of IoT solutions in various applications.

Dr.S.Srinivasan Dr.S.Srinivasan is working as a Professor in the School of Computer Science and Engineering, Galgotias University, Greater Noida, UP, NCR- Delhi, India. He has completed his Ph.D. in Computer Science and Engineering from Anna University, Chennai and obtained his BE and ME from reputed universities. He has presented and published papers in various National and International Conferences and Journals. He has more than 24 years of experience in the field of teaching. He is expertise in Image Processing, Big Data, Cloud, IOT and Artificial Intelligence.

Dr. Sunil Kumar Dr. Sunil Kumar is an Assistant Professor in the School of Computer Science and Engineering at Galgotias University, Greater Noida, UP, NCR-Delhi, India. He obtained his B.Tech in Computer Science and Engineering from R.G.P.V, Bhopal in 2012, followed by an M.Tech in GIS from NIT Bhopal in 2015. In 2023, he earned his Ph.D. in Computer Science and Engineering from Banasthali Vidyapith, Rajasthan. His research interests include Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning technologies. Dr. Kumar has contributed significantly to the field through numerous publications and is dedicated to advancing innovative solutions in AI and ML.

Dr. Sudeep Varshney Dr. Sudeep Varshney is currently an Associate Professor in the Department of Computer Science and Engineering at the School of Engineering and Technology, Sharda University, India. He obtained his Ph.D. in Computer Science and Engineering from IIT (ISM), Dhanbad, Jharkhand. Dr. Varshney graduated with honors in Computer Science and Engineering from Dr. B.R.A. University, Agra, and holds an M.S. degree in Software Systems from BITS, Pilani. With over 19 years of experience in teaching and administration, he has made significant contributions to the academic community. His expertise spans various areas of computer science, and he is dedicated to fostering innovation and excellence in education and research. Dr. Varshney has also published numerous research papers in reputed journals and conferences, further establishing his prominence in the field.