International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Agentic Ai Powered Cryptographic Blockchain for Secured Data Aggregation in Wsn

Mrs. D. Mohanapriya[1], Dr V. Saravanan[2]

[1]Research Scholar & Assistant Professor, Department of Information Technology Hindusthan College of Arts & Science College, Coimbatore, Tamilnadu, India
[2]Professor & HEAD, Department of Information Technology Hindusthan College of Arts & Science College, Coimbatore, Tamilnadu, India

Abstract
Wireless sensor network (WSN) comprises of randomly distributed sensor nodes for sensing and collecting the information in a particular region and transmit to the base station (BS). Due to increasing large volume of data generated, secured data aggregation process is used to protect data aggregation process with higher communication efficiency. Many classification and existing methods were introduced for performing efficient and secured data aggregation in WSN. However it faced significant challenges to achieve the higher confidentiality and integrity in wireless communication system. In order to address these issues, a novel Agentic AI Powered Cryptographic Hash Blockchain (AAIPCHB) method is introduced for secure data aggregation in WSN. The main aim of AAIPCHB method is to perform secure data aggregation with higher data confidentiality and integrity. The AAIPCHB method includes two major processes namely node classification and secure data aggregation. First, the number of sensor nodes is collected as an input. After that, Agentic AI technique is employed for classifying the sensor nodes as normal nodes or intruders based on energy and trust value and signal strength. After the classification process, the data packets are collected from the normal nodes. Then, Koorde Cryptographic hash Blockchain is used to perform the secure transaction from sensor node to the base station. Koorde Cryptographic hash function generates the hash value for every sensor node data packets using Davies–Meyer compression function for preserving the data from the illegal access. This guarantees the integrity during the data aggregation in WSN. Experimental evaluation is carried out for factors such as classification accuracy, data confidentiality, integrity rate, Packet delivery ratio, data aggregation delay and throughput with respect to number of data packets and sensor nodes. Performance comparison analyses illustrate that the proposed AAIPCHB method improves the classification accuracy, throughput, data confidentiality, integrity rate, packet delivery ratio and minimizes the data aggregation delay.

Keywords: WSN, secure data aggregation, resource optimization, Agentic AI, Koorde Cryptographic hash Blockchain, Davies–Meyer compression function

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of many sensor nodes distributed across a specific region to collaboratively observe physical or environmental parameters. Each node generally includes sensing devices to gather information from their environment and forward it to a centralized base station or sink

for further processing and evaluation. WSNs are applied in numerous fields, including environmental observation, industrial process control, smart farming, defense monitoring, and medical or healthcare applications. However, sensor nodes often operate in hostile environments, they are vulnerable to a variety of security threats. These threats considerably affect the integrity, confidentiality, and authenticity of the aggregated information. Therefore, advanced cryptographic techniques, trust-based mechanisms are often incorporated to enhance security of data aggregation without compromising network performance.

A novel blockchain based secure authentication approach called Blockchain_SecAuth approach was developed in [1] for secure data communication within multi-WSNs. However, diverse security models were not employed to solve the scalability issue. A novel Multi-Level Trust Based Secure Routing with blockchain (MLTSR-BC) model was presented in [2] for secure transmission of data between the nodes. Although the model improves throughput, the integrity performance was not significantly enhanced.

Federated Stochastic Gradient Averaging Ring Homomorphism-based Learning (FSGARH-L) method was developed in [3] for secure data aggregation between sensor nodes with high packet delivery and minimizing packet drop rate. However, hash-based verification was not incorporated to increase the data integrity assurance. Elliptic Curve Cryptography and Triple-Layer Authentication Framework (ECC-TLAF) was introduced in [4] to enhance the security by improve energy efficiency and minimize the latency. However, it failed to improve the framework's scalability for enhancing the thread detection. A novel WSN group encryption algorithm was developed in [5] based on chaos theory and performs data compression. However, improvement of optimization strategies was not employed for efficient data collection to further enhance the security and efficiency of wireless medical sensor networks. A new approach called blockchain and swarm intelligence techniques were developed in [6] to enhance energy efficiency and security. However, the designed technique did not apply the broader range of real-world scenarios. An efficient data collection scheme was introduced in [7] for Wireless Sensor Networks (WSNs) that simultaneously performs the data encryption and expand network lifespan. However achieving higher delivery ratio was major concern. An innovative hybrid framework was developed in [8] that integrate Wild Horse Optimization with fuzzy logic for secure data transmission based on lightweight cryptography. However, the model did not utilize the artificial neural networks to further strengthen WSN security and performance.

A lightweight authentication protocols was presented in [9] for secure data transmission with communication overhead. However, the performance of communication delay was not reduced. An Attribute-Based Encryption and Trust Based Secure Routing Algorithm (ABE-TBSRA) was designed in [10] by integrating the bilinear pairing and Diffie Hellman encryption scheme for improving the security. However, block chain based light weight authentication protocols was not explored for providing better security with optimized energy consumption.

A reinforcement learning-based adaptive encryption framework was developed in [11] to categorize network states into low, moderate, or high threat levels. However, blockchain-based key management technique was not employed to further ensure the integrity. A blockchain-based approach was introduced in [12] for addressing the energy-efficient and secure data transmission. However, AI based predictive modelling approach was not developed for dynamic resource allocation in large scale sensor networks. A lightweight two-tier blockchain framework was developed in [13] for secure and scalable data transmission with minimal overhead. However, adaptive cryptographic selection was not integrated to further enhance the scalability in large-scale IoT deployments. Multipath intrusion detection system

(MIDS) was introduced in [14] for achieving the higher packet delivery ratio (PDR), throughput, and detection accuracy. However, the algorithm failed to enhance security by mitigating various attacks. Quantum based secure and energy-efficient routing protocol was designed in [15] for achieving higher data integrity. However, it failed to integrate machine learning for dynamic optimization and exploring energy harvesting technologies to extend network lifespan.

1.1 Research contribution

The main aim of this paper is to propose a novel AAIPCHB method for secure data aggregation in WSN. The major contribution of the AAIPCHB method is summarized as follows,

- A novel AAIPCHB method is proposed to improve secure data aggregation in WSN. This AAIPCHB method integrates two processes, including node classification and secure hash generation.
- To increase the classification accuracy, AAIPCHB method utilizes the Agentic AI model for categorizing the sensor nodes as normal or intruders based on residual energy, trust and signal strength with radial basis kernel function.
- To improve the secure data aggregation in WSN, Koorde Cryptographic hash Blockchain is constructed to generate the hash value based on Davies–Meyer compression function. Then the hash verification is performed based on Obershelp pattern recognition to verify the data integrity.
- Finally, a widespread simulation is carried out to estimate the performance of AAIPCHB method and other deep learning works.

1.2 Organization of the paper:

The paper is structured into six major sections. Section 2 reviews existing literature and outlines the reviews. Section 3 explains the proposed AAIPCHB method along with its architectural framework. Section 4 presents the simulation environment and discusses the obtained results. Section 5 provides a comparative analysis of different approaches using multiple performance metrics. Finally, Section 6 concludes the paper and summarizes the key findings.

2. Related works

An Adaptive Federated Reinforcement Learning-Hunger Games Search (AFRL-HGS) routing framework was introduced in [16] for scalable, secure, and energy-efficient data transmission. However, transmission delay was not effectively reduced. A lightweight homomorphic encryption (HE) technique was designed in [17] for secure data transmission with lower energy consumption, and improved throughput. However, it did not implement more advanced machine learning models to handle more complex scenarios. Exceptional Key based Node Validation for Secure Data Transmission using Asymmetric Cryptography (EKbNV-SDT-AC) model was introduced in [18] to securely transmit the data from source to destination. However, security levels were not efficiently improved. A new blockchain-based computation model was introduced in [19] for optimizing resource utilization and secure data exchange during active communication among mobile sensors. However, it failed to focus on developing AI algorithms for handling dynamic WSN. An innovative Proxy re-encryption (PRE) scheme was introduced in [20] to enhance the secure communication between nodes within the network and external data server. However, the scalability performance of the scheme was not improved.

A blockchain and transfer learning based framework was developed in [21] for secure IoT data management to process large data volumes effectively and enhance data integrity and accessibility.

Secure data aggregation using authentication and authorization (SDAAA) protocol was introduced in [22] to detect malicious attacks. However, data integrity factors remained unaddressed. An enhanced Rank-Based Key Management for Energy-Efficient Cluster-Based Routing Protocol (RK-EFCRP) was developed in [23] aimed to improve the system's stability, security, and energy efficiency. However, the network lifetime, stability and security of the model was not improved. Blockchain-machine learning (BC-ML) was introduced in [24] to efficiently classify the malicious node with higher accuracy. However it failed to increase the performance and power efficiency. A new Blockchain and Machine Learning based infrastructure (KSI) hash chain was developed in [25] for improving the energy efficiency, packet delivery ratio with minimal delay. However, the model has high computational complexity.

Condition-based distributed privacy-preserving (CDPP) approach was introduced in [26] to preserve the sensor node privacy for protection the network. However, the approach did not implement the blockchain to ensure the data integrity. A blockchain 6G-based wireless network security management model was developed in [27] to improve the data delivery and minimize the delay. However, machine learning techniques were not employed to calculate trust for achieving higher security performance levels. An Efficient Key Distribution for Secure and Energy-Optimized Communication using Bioinspired Algorithms (EKDSOCBA) was designed in [28] to achieve security and energy efficiency. However, it failed to focus on the design of data aggregation approaches for improving the energy efficiency of the network. An innovative blockchain-powered safe energy-swapping protocol was designed in [29] to securely handle excess energy, and prolong the network lifespan. However, it failed to predict dynamic energy constraints. An Improved Type-2 Fuzzy Logic System (IT2FLS) was developed in [30] for improving the secure and energy efficient routing with minimal delay. However, the system did not integrate the advanced machine learning techniques to improve the performance of routing and security threats.

3. Proposal methodology

Wireless Sensor Networks (WSNs) consist of compact sensor nodes incorporated with processing units, power sources, and wireless communication modules. These nodes monitor environmental conditions and transfer the collected data to a sink node. The sink node act as a data collector or aggregator point within a WSN to receive data packets from multiple sensor nodes, combines or processes the collected information, and forwards the aggregated results for further analysis. Despite these improvements, achieving secure data aggregation remains a major challenge due to rising security threats.

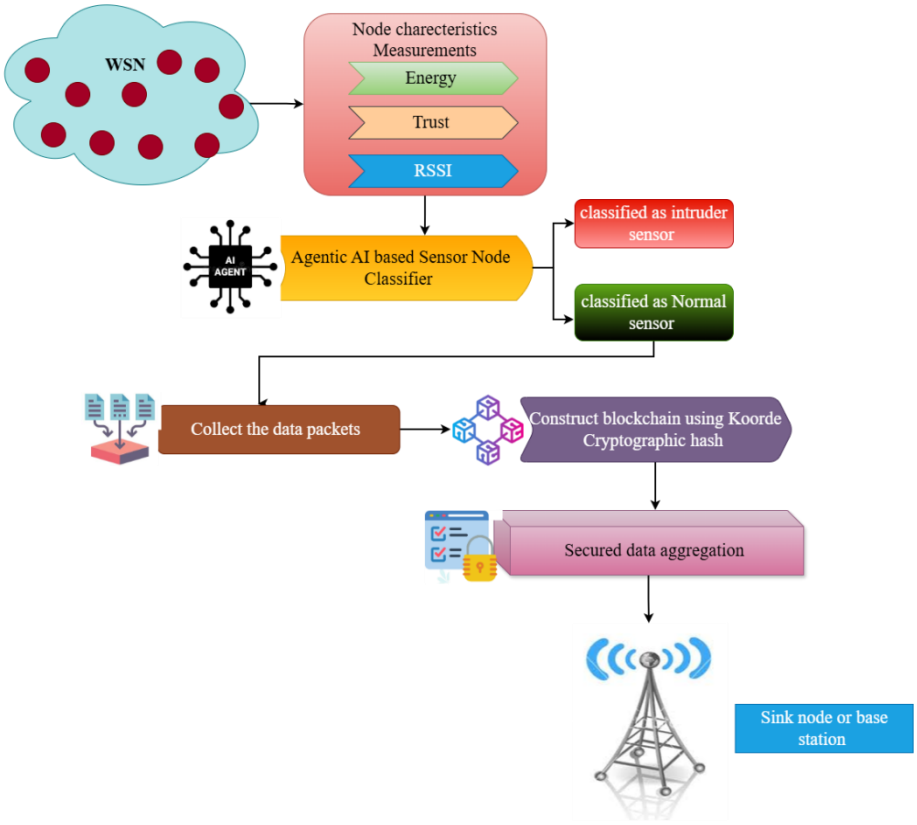

Figure 1 Architecture of the proposed AAIPCHB method

Figure 1 architecture diagram of the proposed AAIPCHB method to obtain secure data aggregation in WSN. The above architecture comprises two major processes namely classification and blockchain construction. The proposed AAIPCHB method utilizes the Agentic AI model for analyzing the sensor nodes characteristics such as energy, Received signal strength indicator (RSSI) and trust level. Based on analysis, the proposed AI model classified the sensor nodes into normal or intruders. Once identified the normal node, sensed data packets are collected from the normal nodes are given to the blockchain technology to perform the secure transaction from sensor node to the base station. Each stage contributes considerably increase the overall performance of the proposed system. A detailed explanation of these processes is provided in the following sections.

3.1 Network model

The proposed AAIPCHB method adopts a network model that is specifically structured to enable secure data aggregation between the sensor nodes and the sink node or base station in WSN. This model consists of a large number of low-power, energy-constrained sensor nodes $SN_i = SN_1, SN_2, SN_3 \ldots SN_n$ distributed in a $M \times M$ squared network area for monitoring and gathering the data packets $Dp_1, Dp_2, Dp_3, \ldots Dp_n$. In order to perform the secure data aggregation, normal sensor nodes are identified based on key characteristics such as energy (E), and trust level (TL) and received signal strength Indicator (RSSI). Followed by, the blockchain is constructed for generating the cryptographic hash 'H' for secure data aggregation at the sink node.

3.2 Agentic AI model

Agentic AI is types of artificial intelligence model that autonomously make decisions without human

interference. In the proposed method, Agentic AI architecture called Deep Q Network (DQN) model is designed for classifying the sensor nodes as normal nodes or intruders within the WSN. Unlike traditional deep learning models, DQN-based classification enabled agents to handle high-dimensional, complex, and massive input with high efficiency. The main aim of DQN is its ability to learn optimal policies directly from raw, high-dimensional sensory input.

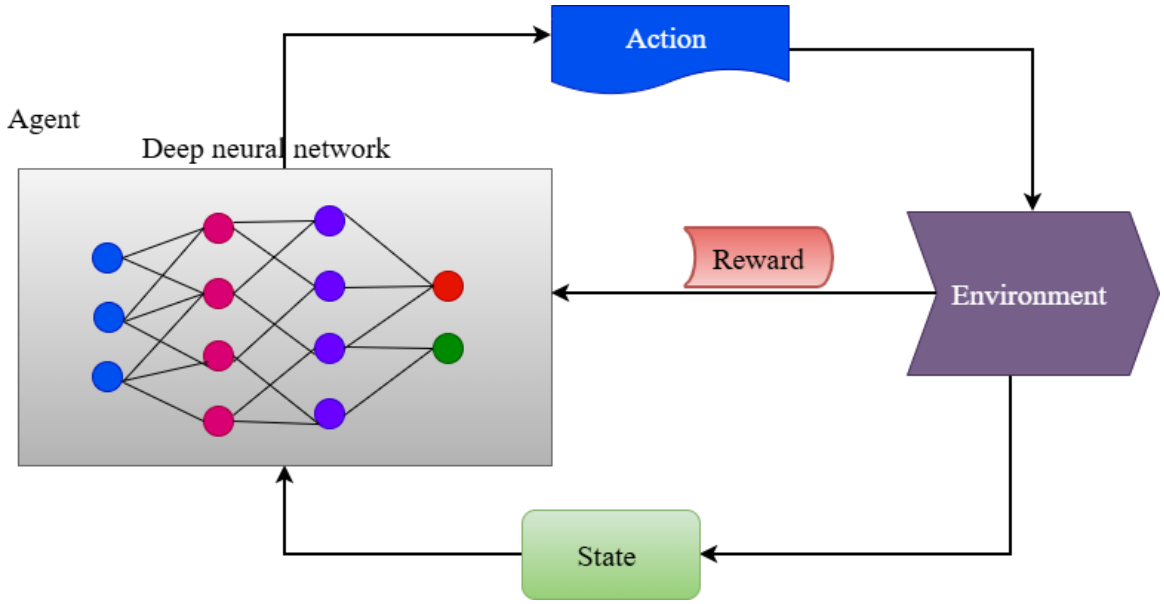

Figure 2 schematic structure of Deep Q Network model

Figure 2 illustrates the schematic structure of the proposed Deep Q Network model developed for accurate classification of the sensor nodes within WSN. As illustrated in the figure, the system considered as an number of sensor nodes as its input. These nodes are evaluated to determine their capacity based on learned decision policies. In the proposed framework, many agents operate using a Deep Q Network model. Each agent cooperates with the surrounding environment and constantly enhances its decision-making policy through knowledge. The main aim of Deep Q Network is to direct agents toward selecting the most suitable actions within a given environment by receiving the maximum cumulative rewards received as feedback.

The main structure of the Deep Q Network includes five important factors namely the agent, environment, states, actions and rewards. The agent is the decision-maker that performs actions. The environment returns a reward in the form of feedback to enhance the accuracy of classification. Actions are the selections of the agent to make a decision. A state indicates the present current condition of the system. A reward is the feedback sent by the environment. Correct predictions are assigned positive rewards, while incorrect predictions result in negative rewards.

By applying Deep Q Network, Q-values are initialized randomly with state-action pair.

Q: (s, a) (1)

Where, 'Q' value initialized with state-action pair(s, a). For each time step, the agent chooses an action i.e. classification tasks and received a reward from the environment and shifts to a new state followed by updating the initial Q-value.

To begin with, the agent in the Deep Q Network model chooses the action as a classification tasks by utilizing the deep neural network model with number of sensor nodes. The proposed Deep Q Network considers the training set $\{SN_i, Y_k\}$ where SN_i indicates number of sensor nodes and Y_k indicates a classification results.

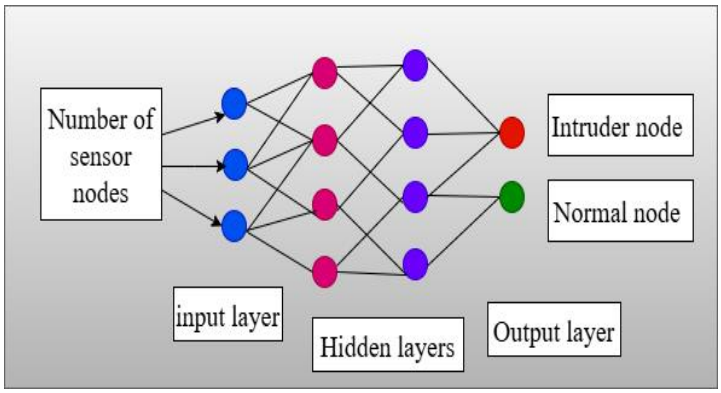

Figure 3 structure of Deep Q Network model

Figure 3 reveals the construction of Deep Q Network model comprises of three major layers namely input, numerous hidden layers and output layer. The input layer receives the system inputs, specifically the number of sensor nodes. Between the input and output layers are the hidden layers, which consist of neurons (or nodes) that process the incoming sensor nodes by applying weighted connections. The output layer then generates the final classification results based on the computations performed in the hidden layers.

In input layer, each neuron receiver the number of sensor nodes and transfers it to the hidden layer where the weighted sum is computed based on weights and biases. In the hidden layer, each neuron resolves a weighted sum of inputs as follows,

$Q = \sum_{i=1}^{n} SN_i * w_{ih} + B$ (2)

Where, Q symbolizes a weighted sum output, SN_i designates a sensor nodes, w_{ih} designates a weight between neuron in input layer and hidden layer, and B represents a bias. Let us consider input i.e. sensor nodes $SN_1, SN_2, SN_3 \ldots, SN_n$'.

At the beginning of the process, all sensor nodes are initially considered to hold the same amount of energy. However, as it performs sensing and monitoring activities, their energy gradually depletes. Therefore, the residual energy typically indicates the remaining energy of the sensor node is computed as follows,

$EN_{res}\ (SN_i) = EN\ _T\ (SN_i) - EN_{con}^{SN_i}$ (3)

Where, $EN_{res}\ (SN_i)$ indicates the residual energy of i^{th} sensor node,$EN\ _T\ (SN_i)$ represents total energy of i^{th} sensor node, $EN_{con}^{SN_i}$ denotes an energy consumed by the i^{th} sensor node.

The direct trust value of a node is calculated as the ratio of successful data transmissions to the total number of transmissions, includes both successful and unsuccessful attempts. This value reflects the reliability and trustworthiness of the node. Mathematically, the direct trust value is expressed as follows:

$T^{SN} = \left[\frac{S_{DT}}{S_{DT}+US_{DT}}\right]$ (4)

Where, T^{SN} indicates a trust of sensor nodes, S_{DT} symbolizes a successful data transmission, US_{DT} indicates an unsuccessful data transmission.

Signal strength represents the power level of a radio signal received by a vehicle node from a transmitter, usually measured in dBm. It is an important indicator of connection reliability and data transmission speed. The signal strength of a vehicle node is calculated using the Friis transmission equation, which is expressed as follows:

$RSSI(SN) = Tr_i * g_t * g_r * \left(\frac{\lambda}{4\pi D}\right)^2$ (5)

Where, $RSSI(SN)$ represents a received signal strength or power of i^{th} sensor nodes, Tr_i transmitted signal strength of i^{th} sensor nodes, g_t and g_r denotes a gain of transmitter and receiver antenna, λ denotes the wavelength of the signal, D denotes the distance between the transmitter and receiver.

The RBF kernel function calculates the similarities between estimated resource and threshold.

$$\tau_k = exp\left[-\frac{|SN_i(R)-\delta|^2}{2\sigma^2}\right] \quad (6)$$

Where, τ_k denotes a RBF kernel function, $SN_i(R)$ indicates a sensor node resources i.e , residual energy, trust of sensor nodes, received signal strength, δ denotes a threshold, σ denotes a deviation function. Based on the kernel function, the kernel function provides the similarity results from '0' to '1. From the (6), the classification outcome such as normal and intruder are correctly detected.

$$\tau_k = \begin{cases} 0\,; & Intruder \\ 1\,; & normal \end{cases} \quad (7)$$

Where, if the kernel function 'τ_k' returns '1', the node are classified as normal. Otherwise, the nodes are classified as intruder. In this way, accurate intrusion detection is performed.

Therefore, the classification outcomes are observed at the output layer as given below,

$$Y = f\,(h_t * w_{ho}) \quad (8)$$

Here, Y represents a classification output, f represents the sigmoid activation function provide the two class classification results such as normal sensor nodes and intruder sensor nodes, w_{ho} represents a weight between neuron in hidden layer and output layer, h_t denotes a hidden layer output.

For each classification outcome, the error rate is measured by computing the squared difference between the actual result and the predicted classification.

$$CE = [Y_{Act} - Y_{Obs}]^2 \quad (9)$$

Where, 'CE denotes the classification error rate, Y_{Act} denotes the actual classification results, Y_{Obs} indicates the observed classification output.

After each action i.e. classification result, the environment provides a reward that reflects the agent's performance. This reward acts as feedback, allows the agent to fine-tune its decisions and increase the accuracy of classifications. Positive rewards are given for correct classifications, while incorrect classifications gain negative rewards.

$$R\,(s,a) = \begin{cases} min\ ; high\ CE \\ max\ ; Less\ CE \end{cases} \quad (10)$$

Where, $R\,(s,a)$ represents the reward for taking action 'a' in current state's', CE represent the classification error rate. A higher CE, representing larger error, results in a lower reward, whereas a lower CE, reflecting more accurate classification, provides a higher reward. Based on that reward allocation, initial Q value is value for the current state–action pair (s,a) updated using following expression.

$$Q^{updated}\,(s,a) = Q_t\,(s,a) + \eta\,[\,R\,(s,a) + \tau.\ max\ Q\,(s_{t+1},a_t) - Q_t\,(s_t,a_t)] \quad (11)$$

Where, $Q^{updated}\,(s,a)$ designates an updated Q-Value, $Q_t\,(s,a)$ represents a current Q value, η denotes a learning rate ($0<\eta<1$), $R\,(s,a)$ denotes a reward, τ indicates a discount factor only slightly lesser than 1, $max\ Q\,(S_{t+1},A_t)$ indicates a maximum Q-value of the next state for a particular action, (s,a) indicates a current action and state pair respectively. This process is repeated until it reaches the maximum number of iterations. The algorithm process of Agentic AI model is given below.

// Algorithm 2: Agentic AI based node classification

Input: Number of sensor nodes $SN_1, SN_2, SN_3 \ldots, SN_n$

Output: normal and intruder node classification

Begin

1: Collect sensor nodes $SN_1, SN_2, SN_3 \ldots, SN_n$
2. Initialize the Q table with state and action pair Q: (s, a)
3. **While** $(t \leq Max\_t)$ **do**
4. **For each pair** (s, a)
5. Apply the deep Q neural network
6. Sensor nodes are given as input layer
7. Measure the weighted sum using (2)
8. **For each** Sensor node
9. Measure the residual energy' using (3)
10. Compute the trust value using (4)
11. Compute the RSSI using (5)
12. Measure radial kernel similarity using (6)
13. **If** $(\tau_k = 1)$ **then**
14. Sensor nodes are classified as normal
15. **else if**$(\tau_k = 0)$ **then**
16. Sensor nodes are classified as intruder
17. **End if**
18. Classification results are observed at output layer using (8)
19. **For each** classified results
20. **Compute** the error using (9)
21. **If** $(min\ CE\ )$ **then**
22. Assign maximum reward '$R\ (s, a)$'
23. **else**
24. Assign minimal reward $R\ (s, a)$
25. **End if**
26. Update the Q table value '$Q^{updated}\ (s, a)$' using equation (11)
27. **Increment** $t = t + 1$
28. Go to step 3 until it converges
29. **End For**
30. **End while**
31. **Return (**accurate classification results**)**

End

Algorithm 1 presents Agentic AI for accurate classification of sensor nodes in WSN. The algorithm begins by initializing the Q-values for all different state-action pairs. The input layer receives the sensor nodes from the action space. For each sensor node, weights and biases are computed in hidden layer. The energy, trust and signal strength of each vehicle node is then evaluated. To perform classification, radial kernel similarity is measured. Sensor nodes with resource capacities below a specified threshold are classified as intruder, while those exceeding the threshold are classified as normal. The output layer uses a sigmoid activation function to generate the final two-class classification results. For each classification outcome, the error rate is calculated, and rewards are assigned based on the accuracy of the

prediction. The Q-values are iteratively updated until the model converges. Finally, the process produces precise and reliable node classification results for secure data transmission.

3.3 Koorde Cryptographic hash Blockchain

After the classification process, data packets are collected from the normal nodes and it is secured using blockchain technology. Blockchain is a decentralized, distributed, and permanent digital ledger technology that records transactions, ensuring data security without dependence on a central authority. In the chain, blocks of data are cryptographically connected that ensures privacy-preserving individual's data is accessible only to authorized individuals, thereby preserving the data privacy.

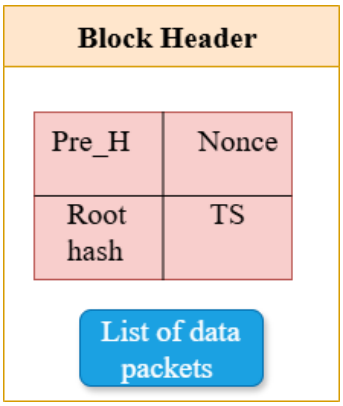

Figure 4 structure of blockchain

Figure 4 demonstrates blockchain, depicting the series of blocks that generate a chain among a limited group of normal sensor nodes to protect the data packets. Each block comprises of various components such as a block header, cryptographic hash of the previous block (Pre_H), timestamp (TS), and root hash. Then the proposed blockchain utilizes the Koorde Cryptographic function for each data packets using Davies–Meyer Compression to generate the hash value. The hash of the previous block (p_hash) is used for block confirmation. Time steps (T_s) refers to the time when the block was created.

Koorde is a distributed system that generates the hash function for each data packets and stored into a blockchain in the form of a De Bruijn graph. The De Bruijn graph is a directed graph model which consists of vertices and edges. The vertices are called as data packets that are connected by edges called connections. In a graph-based network model, the vertices represent data packets, while the edges denote the connections between them. Each vertex corresponds to an individual packet containing information, and an edge indicates that there is a link between two packets. This representation allows the data transmission process to be visualized as an interconnected structure, where packets cooperate, propagate, or depend on one another through defined network links.

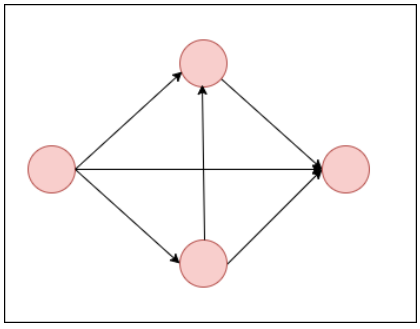

Figure 5 De Bruijn graph

The main advantage of De Bruijn graph is used for the process of retrieving the data packets quickly from a blockchain. The hash function is generated using Davies–Meyer Compression function

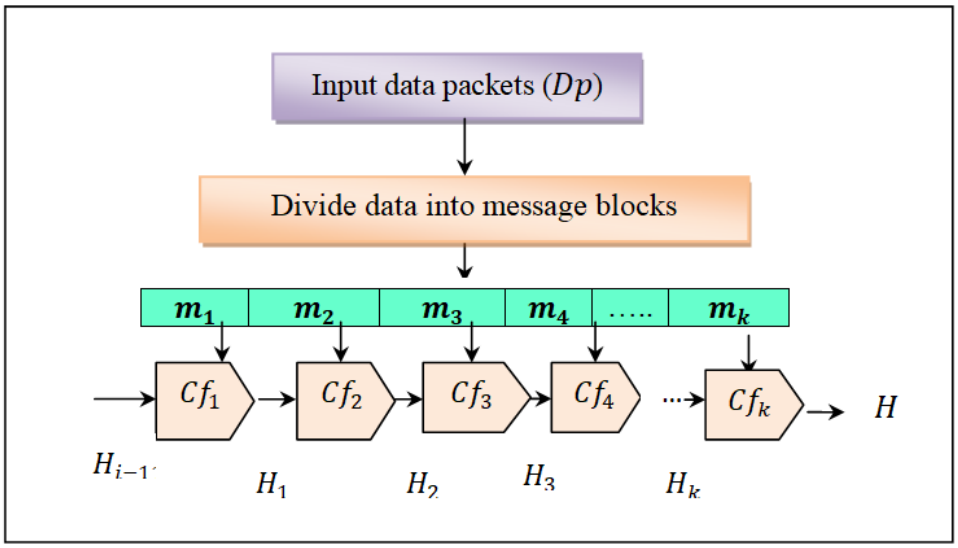

Figure 6 Davies–Meyer Compressions

Figure 6 illustrates the structure of the Davies–Meyer Compression to generate the output hash 'H'. As shown in figure 6, $Cf_1, Cf_2, Cf_3, Cf_4, .. Cf_k$ indicates a Davies-Meyer block compression function. Let us consider the input data packets $Dp_1, Dp_2, Dp_3, \ldots Dp_n$ divided into 'k' number of message blocks as follows.

$Dp \rightarrow m_1, m_2, m_3, \ldots m_k$ (12)

Then the message blocks with fixed size is given as input to the compression function.

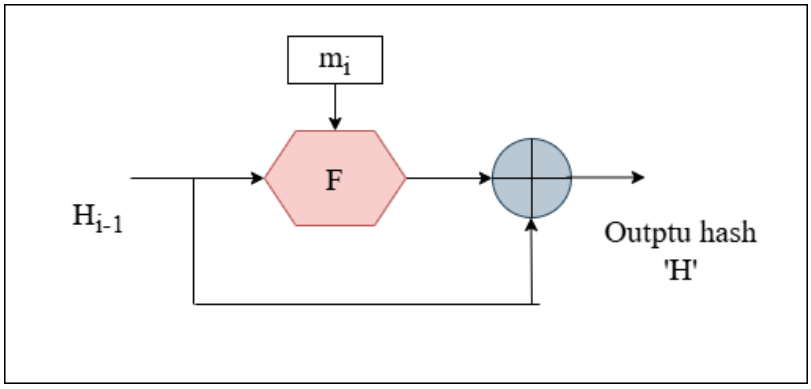

Figure 7 hash generation

Figure 7 portrays the Davies-Meyer block compression function to generate the hash value for each data packets for secure data aggregation at the sink node. The compression function obtains the input message block 'm_i' with fixed size and the previous hash value 'H_{i-1}' (i.e.Pr_H). In the first round, there is no previous hash value available, the algorithm is configured to utilize a predefined constant as the initial hash value. The output of the compression function is expressed as given below,

$H_i = F_{m_i}(H_{i-1}) \oplus H_{i-1}$ (13)

Where,H_i indicates a hash of the current message block,m_i indicates the message block, H_{i-1} denotes a hash of the previous round, '$\oplus$' represents an XOR which is the logical operator, F indicates a block cipher to encrypt a block of data packet to improve the security. The output of the final compression function 'Cf_k' is used to generate the final hash value. In this way, hash value is generated for all the

data packets and it stored into the blockchain. This helps to improve the confidentiality of the data packets while transferring from sender node to sink node.

3.3.1 Hash verification

After the blocks creation, the base station or sink node initiates a verification process to ensure that only valid transmissions are recorded on the blockchain, thereby preserving the network's security and integrity. The node authorization method based on block verification, where each transaction and block is validated to confirm consistency. This validation procedure strengthens the trustworthiness, consistency, and overall security of the blockchain system.

Hash validation plays a vital role in blockchain operations by confirming that every newly generated block conforms to the rules established by the consensus mechanism. This step protects the correctness and authenticity of the computed hash values. The network specifies explicit consensus criteria for validating the hash output, including a requirement that the length of the produced hash must match the maximum allowable size.

In the proposed blockchain system, Obershelp pattern recognition technique is integrated into the verification stage to further support data consistency and detects irregularities. Together, these validation procedures, sensitive organizational data is processed and maintained in a reliable and protected manner.

Obershelp pattern recognition is used to determine the similarity between two characters or patterns. The main aim of this algorithm measures the relationship between two patterns and providing an output score between zero and one. A value of 1 denotes a complete match between the two patterns, whereas a value of 0 indicates no similarity between them. The resulting score represents the level of similarity, where values approaching 1 correspond to greater similarity and values nearer to 0 reflect lower similarity.

The generated hash size ' $[H\ (Dp)]$' using Davies-Meyer compression for corresponding data packets 'Dp' and the maximum allowable hash size or length specified by the blockchain network denoted by '$Dp_{size}(H)$ are given to the input to the Obershelp pattern recognition. It is mathematically expressed as follows,

$$OPR = 2 * \frac{Matched\ patterns}{|H\ (Dp)]||Dp_{size}(H)|} \quad (14)$$

Where OPR denotes an Obershelp pattern recognition, Ms_m denotes a matched patterns, $H\ (Dp)$ indicates a size of hash value generated by cryptographic function, $Dp_{size}(H)$denotes a maximum allowable hash size specified by the blockchain network, $|H\ (Dp)|$ and $|Dp_{size}(H)|$ represents the cardinality of set i.e. number of patterns in hash length or size. The score provides the output values between zero and one. Based on the computed value, a score of 1 signifies that the generated hash length exactly matches the maximum permitted hash length, indicating full conformity between the two patterns. Conversely, a score of 0 reflects a complete mismatch, meaning the generated hash length does not match with the allowable limit.

$$Z = \begin{cases} OPR > T\ ; & block\ valid \\ OPR < T\ ; & not\ valid \end{cases} \quad (15)$$

Where, Z denotes an output function, OPRdenotes a validation score or Obershelp pattern recognition output, T denotes a threshold. If the validation score exceeds the threshold, the block is considered as valid. Otherwise, if the validation scores lesser the threshold, the block is identified as invalid. The valid blocks are used to ensure that only correct, trustworthy data becomes part of the permanent ledger. This

helps to maintaining security, integrity of the data. In this way, the proposed technique performs secure data aggregation in WSN. The step-by-step procedure for hash generation is outlined as follows,

// **Algorithm 2 : Koorde Cryptographic hash Blockchain**
Input: Number of normal sensor nodes $SN_1, SN_2, SN_3 \ldots, SN_n$, data packets $Dp_1, Dp_2, \ldots Dp_m$, **Output:** Secure data aggregation
Begin **Block generation** **Step 1**: **For each** normal sensor nodes 'SN' **Step 2: For each** data packets 'Dp **Step 3:** Convert data into message blocks $m_1, m_2, m_3, \ldots m_k$ using (12) **Step 4: End for** **Step 5: For each** message block 'm_k' **Step 6:** Generate hash ' H 'using (13) **Step 7**: **End for** **Step 8**: **for each** Generate hash size ' $[H\ (dp)]$ **Step 9**: **for** maximum allowable hash size '$Dp_{size}(H)$' **Step 10:** Measure Obershelp pattern recognition 'OPR' using (14) **Step 11:** $\boldsymbol{If}\ (OPR' = 1)\ \boldsymbol{then}$ **Step 12:** Generated hash size matched with allowable hash size **Step 13**: Block is said to be valid **Step 14**: **else** **Step 15:** Generated hash size not matched with allowable hash size **Step 16:**Block is said to be invalid **Step 17:End if** **Step 18**:**End for** **Step 19:End for** **Step 20: End for** **End**

Algorithm 2 describes the various processing steps involved in secure hash generation for each data packets using Koorde Cryptographic hash Blockchain. In the proposed blockchain, the block generation process begins for all normal sensor nodes and their data packets. The input data packet is partitioned into message blocks of equal size, providing a structured format for secure hashing. The Davies-Meyer block compression function is then applied to generate the hash value for each data packets. The generated hash is stored on the blockchain server, enhancing data confidentiality. Next, Obershelp pattern recognition is used to verify the hash, considering the maximum allowable size of the hash. If the validation score exceeds the threshold, the block is identified as valid. Otherwise, the block is identified as invalid. By allowing only verified blocks to be linked in the chain, the system prevents tampering, ensures data integrity, and enables secure and trustworthy data aggregation within the WSN environment.

4. Simulation Setup

In this section, simulations of three different methods namely the proposed AAIPCHB and two existing methods referenced as Blockchain_SecAuth approach [1], and MLTSR-BC [2] are implemented using

the NS-3 simulator A total of 500 sensor nodes are deployed within a square area measuring 1100 m × 1100 m. The Random Waypoint mobility model is employed to simulate node movement and to facilitate secure data aggregation in the wireless sensor network (WSN). The total simulation time is set to 100 seconds. To further improve energy efficiency and ensure secure data transmission, the Dynamic Source Routing (DSR) protocol is implemented. The simulation parameters along with their respective values are presented in Table 1.

Table 1 Simulation Parameters

Simulation parameters	Value
Simulator	NS3
Network area	1100m * 1100m
Number of sensor nodes	50, 100, 150, 200…500
Number of data packets	100, 200, 300, ….1000
Protocol	DSR
Simulation time	100sec
Mobility model	Random Way Point model
Nodes speed	0-20m/s
Communication range of a sensor nodes	30m
Number of runs	10

4.1 Simulation implementation results

In this section, the different process of AAIPCHB method is discussed with screenshot in detail. First, 50 sensor nodes are randomly distributed in $1100 * 110m$ squared region for collecting the environmental data.

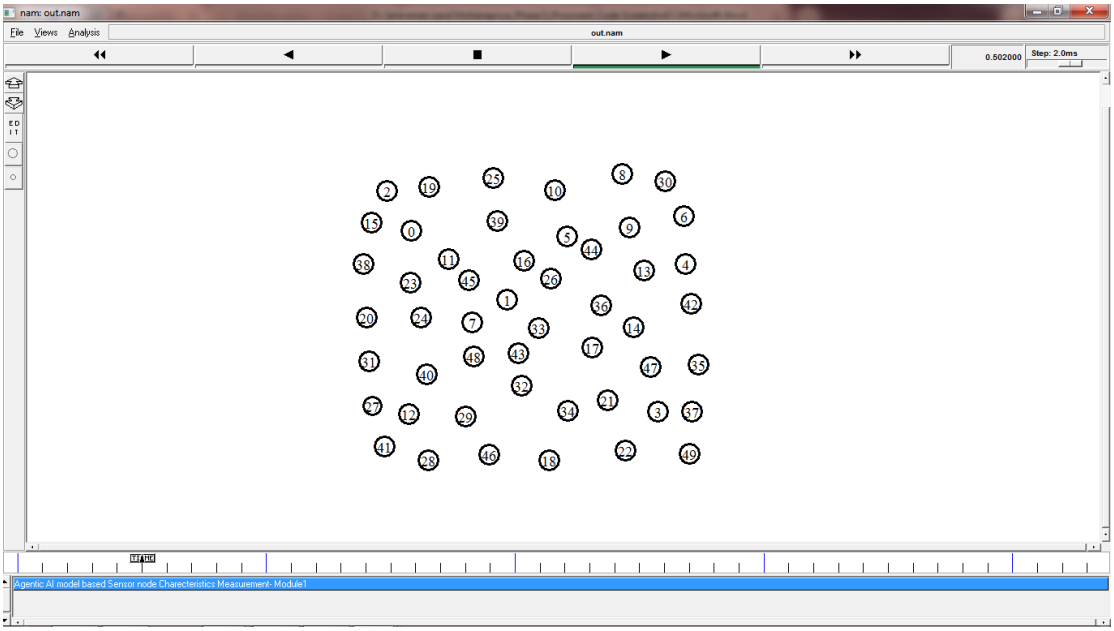

Figure 8 deployments of sensor nodes

After distributing the sensor nodes within the particular network region, residual energy, trust and signal strength are computed to identify the normal node and intruder node by applying an agentic AI model as shown in figure 9.

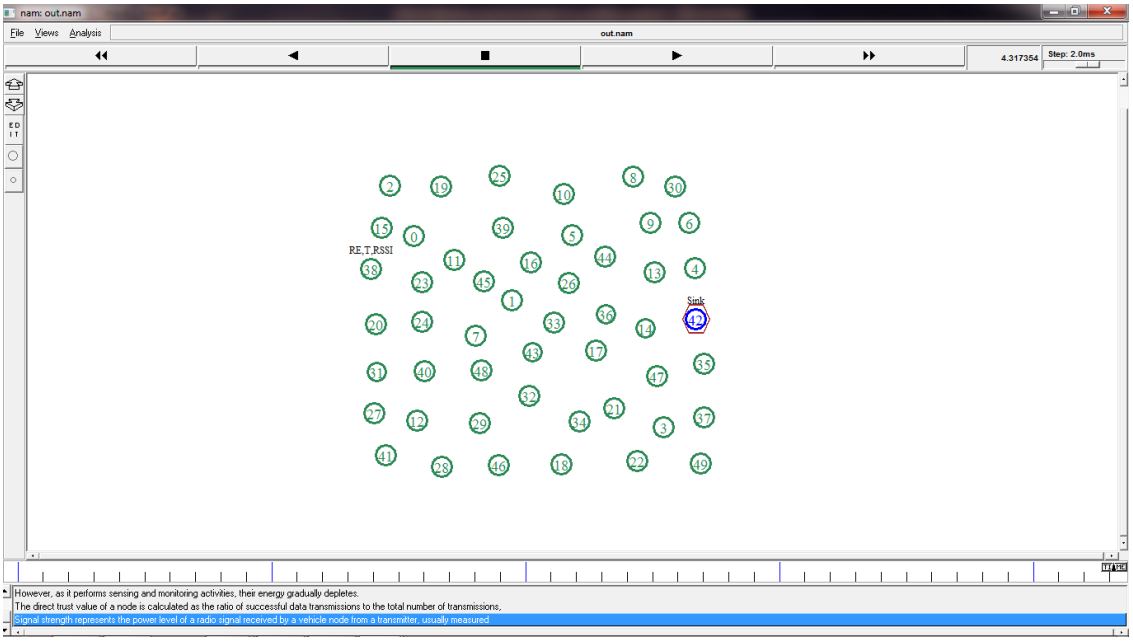

Figure 9 residual energy, trust and signal strength estimation

After classifying the sensor nodes, agentic AI model is employed for classifying the legitimate and intruder sensor nodes within WSN.

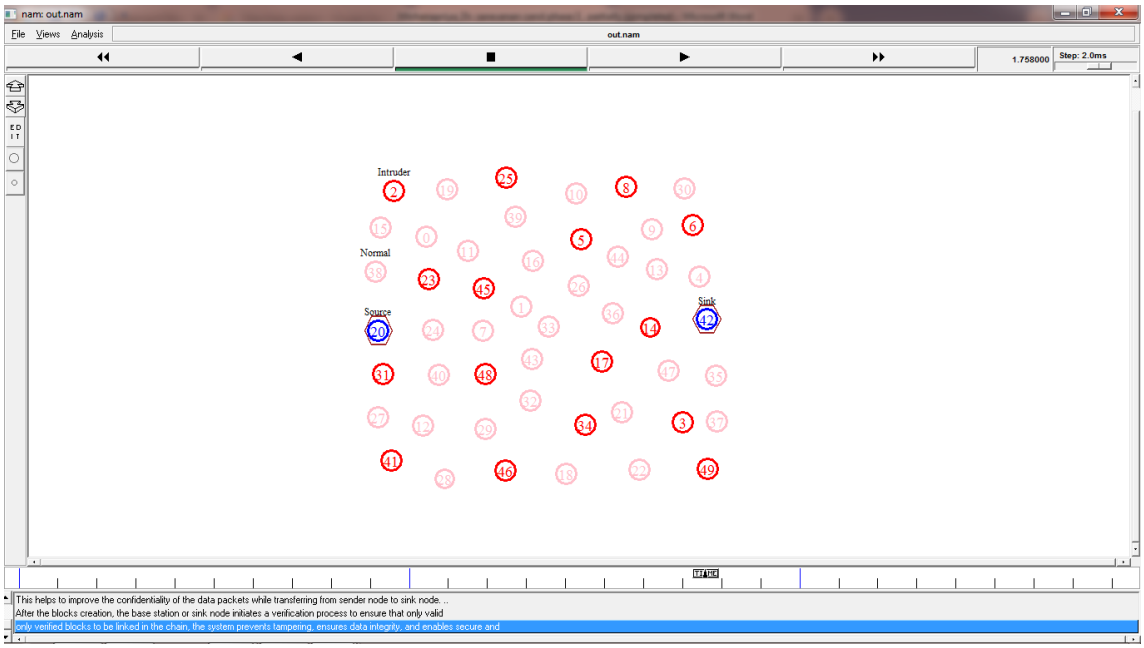

Figure 10 sensor nodes classification

Figure 10 demonstrates 50 sensor nodes randomly deployed within the network area. The nodes are represented using different colors to indicate their roles and status. Red circles indicating normal nodes whereas pink coloured node classified as Intruder for detecting ensuring data integrity.

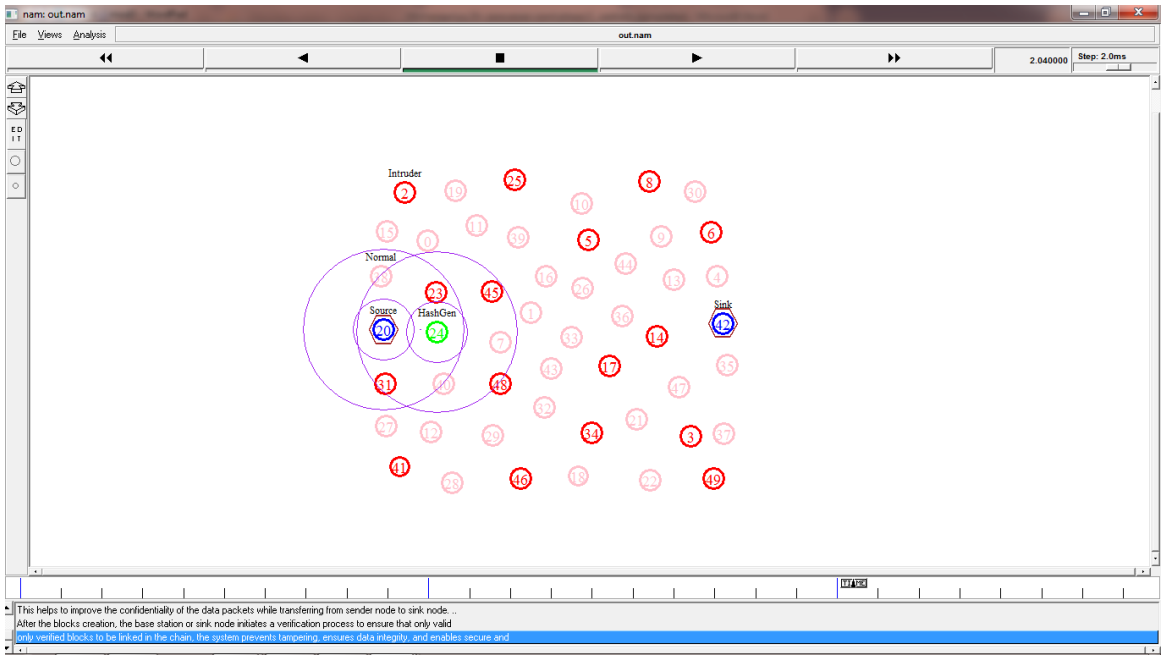

Figure 11 Koorde Cryptographic hash Blockchain

After the classification, data packets are gathered from the normal nodes. Subsequently, a Koorde-based cryptographic hash blockchain mechanism is applied to enable secure data transmission from the sensor nodes to the base station. The Koorde cryptographic hash function computes a unique hash value for each sensor node's data packet using the Davies–Meyer compression function. This approach ensures data integrity throughout the aggregation process in the wireless sensor network (WSN).

Finally, secure data transmission is performed between the sender and sink node.

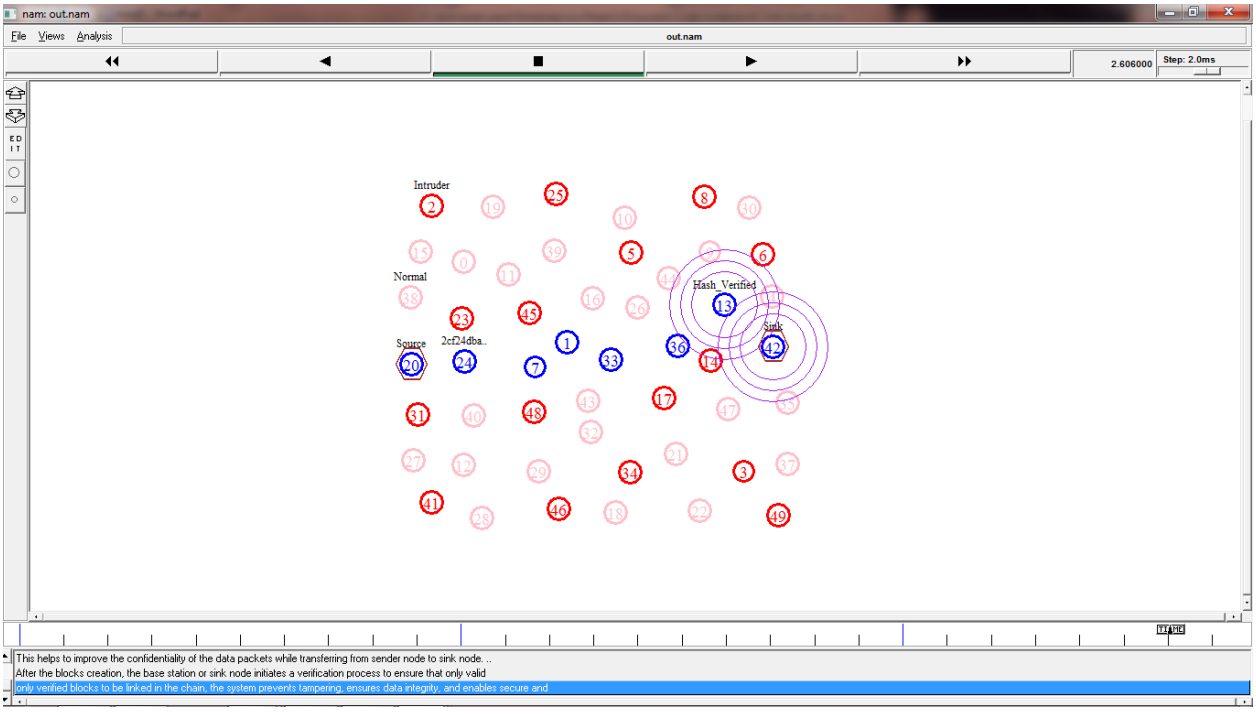

Figure 12 blockchain-based hash verification

This suggests that a blockchain-based hash verification mechanism is applied for secure data transmission and integrity verification within a wireless sensor network.

5. Performance comparison analysis

This section offers a comparative analysis of AAIPCHB by comparing it with established state-of-the-art methods, namely Blockchain_SecAuth approach [1], and MLTSR-BC [2]. The performance evaluation uses metrics such as classification accuracy, data confidentiality, integrity rate, Packet delivery ratio, data aggregation delay and throughput. The performance of AAIPCHB method is compared to existing model relating to these metrics is illustrated through tables and graphical representations.

5.1 Evaluation metrics

Classification accuracy: It measured as the ratio of correctly classified the sensor nodes into normal or intruders to the total number of sensor nodes distributed within the WSN. The mathematical formula for calculating the accuracy is given below,

$$CA = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) * 100 \quad (16)$$

Where, CA denotes a classification accuracy, TP (True Positive) represents the number of correctly classified normal nodes, TN (True Negative) denotes the number of correctly classified intruder nodes, FP (False Positive) refers to intruder nodes incorrectly classified as normal nodes, and FN (False Negative) represents normal nodes incorrectly classified as intruder nodes. Accuracy is measured as a percentage (%).

Data confidentiality rate: it refers to the ratio of number of data packets accessed by authorized normal nodes. Mathematically, the confidentiality rate is computed as follows,

$$DCR = \sum_{j=1}^{m} \left[\frac{DANN}{Dp_j}\right] * 100 \quad (17)$$

Where, DCR represent the data confidentiality rate, m denotes the number of data packets 'Dp', $DANN$ indicates a data packets accessed by authorized normal node. The confidentially rate is measured in percentage (%).

Data integrity rate: The integrity rate is measured as the number of data packets that have not been changed or altered by any unauthorized intruders during the data aggregation. The the integrity rate is mathematically computed as follows,

$$DIR = \sum_{j=1}^{m} \left[\frac{DNA}{Dp_j}\right] * 100 \quad (18)$$

Where, DIR indicates a data integrity rate,Dp_j denotes the number of data packet, DNA denotes a number of data packets not altered by any intruders. It is measured in the unit of percentage (%).

Packet delivery rate: Packet delivery performance measures the effectiveness of the proposed approach in which number of reliable data packets are aggregated at sink node without. Packet delivery ratio is measured as follows,

$$PDR = \sum_{j=1}^{m} \left[\frac{DpD}{Dp_j}\right] * 100 \quad (19)$$

Where PDR refers to a Packet delivery ratio, DpD the data packets correctly delivered at the sink node and $DP_j\ sent$ indicates a data sent. The ratio is measured in terms of percentage (%).

Data aggregation delay: it measures the difference between the expected arrivals and the observed arrival time of data packets at sink node. The formula for calculating the Data aggregation delay is expressed as follows,

$$DAD = Time\ (EAT)\ - Time\ (OAT) \quad (20)$$

Where, DAD denotes an aggregation delay, $Time\ (EAT)$ denotes a expected time of j^{th}data packet

aggregated at the sink node,$Time\ (OAT)$ denotes a time of j^{th}data packet observed at the sink node. It is measured in milliseconds (ms).

Throughput: it is defined as the rate of successful data transmission over a communication network within a specified time period. It is typically measured in bits per second (bps). The formula for calculating throughput is given as follows:

$$THP = \left[\frac{Succ\_Trans\_\ data\ packet\ (bits)}{time\ (s)}\right] \quad (21)$$

Where, THP represents a throughput, $Succ\_Trans\_\ data\ packet\ (bits)$ indicates a successful transmission of data packets in bits in one seconds (Bps).

5.2 Performance Comparison Analyses

This section provides a comparative performance analysis of AAIPCHB model against existing approaches, including Blockchain_SecAuth approach [1] and MLTSR-BC [2]. AAIPCHB by comparing it with established state-of-the-art methods

5.2.1 Classification accuracy

This section describe the classification accuracy component of comparative performance analysis of AAIPCHB model against existing approaches, including Blockchain_SecAuth approach [1] and MLTSR-BC [2] with respect to number of sensor nodes.

Table 2 comparison analysis of classification accuracy

Number of sensor nodes	Classification accuracy (%)		
	Proposed AAIPCHB	Existing Blockchain_SecAuth approach [1]	Existing MLTSR-BC [2]
50	96	92	90
100	97.23	92.23	90.63
150	96.85	92.56	90.52
200	96.26	92.45	90.05
250	96.43	92.74	90.44
300	96.74	92.63	90.41
350	96.82	92.45	90.63
400	96.32	92.36	90.55
450	96.42	92.74	90.45
500	96.56	92.63	90.66

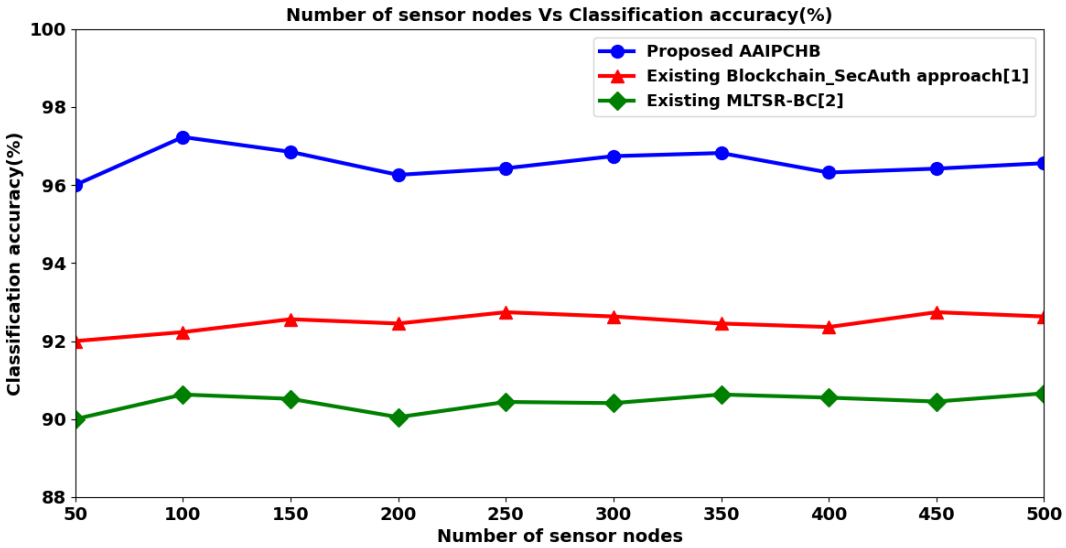

Figure 13 Graphical chart of classification accuracy

Figure 13 demonstrates a graphical assessment of classification accuracy among three approaches namely the proposed AAIPCHB method against existing approaches, including Blockchain_SecAuth approach [1] and MLTSR-BC [2]. In the figure, the x-axis represents the number of sensor nodes ranges from 50 to 500, while the y-axis portrays the corresponding classification accuracy. The results obviously illustrate that the AAIPCHB method consistently achieved higher accuracy in sensor node classification than the baseline methods. For example, with 50 sensor nodes, the AAIPCHB method obtained an accuracy of 96%, whereas methods [1] and [2] achieved 92% and 90%, respectively. The average value of ten observed tests indicates that the AAIPCHB method exhibited an average improvement of 4% and 7% when compared to [1] and [2] respectively. This greater performance is achieved owing to the integration of an agentic AI architecture, which increases the model's ability to accurately analyze the sensor node characteristics such as residual energy, trust and RSSI. During the analysis, the model utilizes a Deep Q network model classified the sensor node into normal or intruder nodes with higher accuracy.

5.2.2 Data confidentiality rate

This section describe the Data confidentiality rate using three methods namely AAIPCHB method against existing approaches, including Blockchain_SecAuth approach [1] and MLTSR-BC [2] with respect to number of data packets.

Table 3 comparison analysis of data confidentiality rate

Number of data packets	Data confidentiality rate (%)		
	Proposed AAIPCHB	Existing Blockchain_SecAuth approach [1]	Existing MLTSR-BC [2]
100	98	94	92
200	98.23	94.12	92.36
300	98.48	94.32	92.41
400	98.36	94.42	92.45

500	98.25	94.36	92.74
600	98.43	94.33	92.34
700	98.36	94.54	92.33
800	98.74	94.36	92.25
900	98.62	94.22	92.16
1000	98.55	94.18	92.11

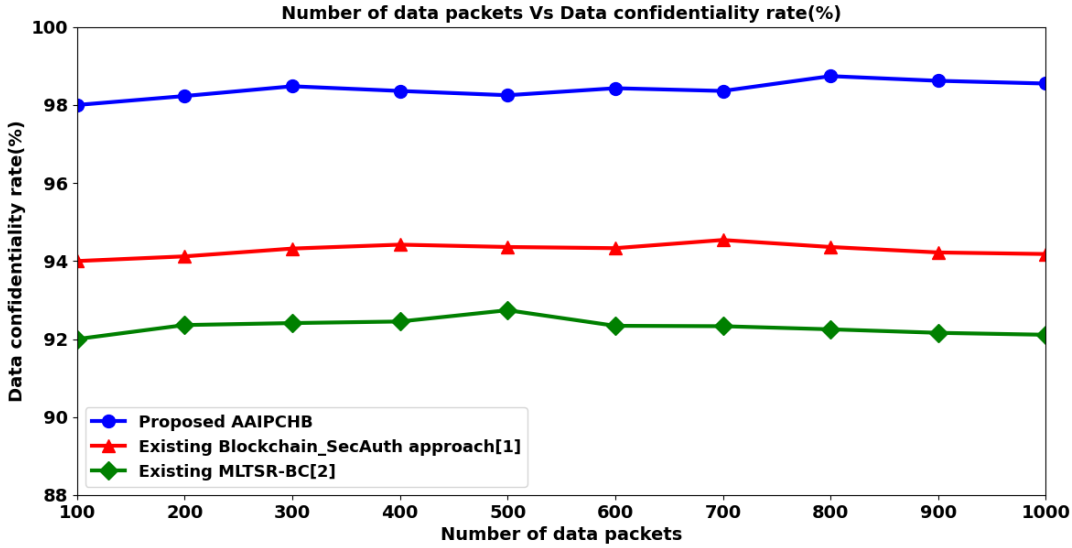

Figure 14 Graphical chart of data confidentiality rate

Figure 14 demonstrates the graphical results of the confidentiality rate using proposed AAIPCHB method compared with two existing approaches Blockchain_SecAuth approach [1] and MLTSR-BC [2]. The assessment is carried out using input data packets ranging from 100 to 1000 data. The results indicate that the AAIPCHB method consistently preserves higher data confidentiality during data aggregation using Koorde Cryptographic hash Blockchain compared to the other methods. For example, with 100 data packets, the AAIPCHB method achieved a confidentiality rate of 98%, whereas methods [1] and [2] recorded 94% and 92%, respectively. Similar results were observed across the remaining nine results. The average of ten performances results were over all ten test cases, AAIPCHB method showed an improvement by 4% over [1] and 7% over [2] in confidentiality rate. The superior performance of the AAIPCHB method model is achieved owing to its integrated Koorde Cryptographic hash Blockchain. When accessing the data, the authority nodes to ensure that only legitimate individuals retrieve the information. The illegitimate nodes are accurately identified through the agentic AI model. This security measures significantly enhances the overall confidentiality of the data packets.

5.2.3 Data integrality rate

This section evaluates the data confidentiality rate of the proposed AAIPCHB method and compares its performance with existing methods, specifically the Blockchain_SecAuth approach [1] and MLTSR-BC [2], under varying numbers of data packets.

Table 4 comparison analysis of Data integrity rate

Number of	Data integrity rate (%)

data packets	Proposed AAIPCHB	Existing Blockchain_SecAuth approach [1]	Existing MLTSR-BC [2]
100	97	93	91
200	97.23	93.22	91.52
300	97.16	93.16	91.44
400	97.63	93.41	91.36
500	97.55	93.26	91.41
600	97.36	93.16	91.32
700	97.41	93.25	91.06
800	97.23	93.18	91.31
900	97.34	93.35	91.44
1000	97.21	93.32	91.23

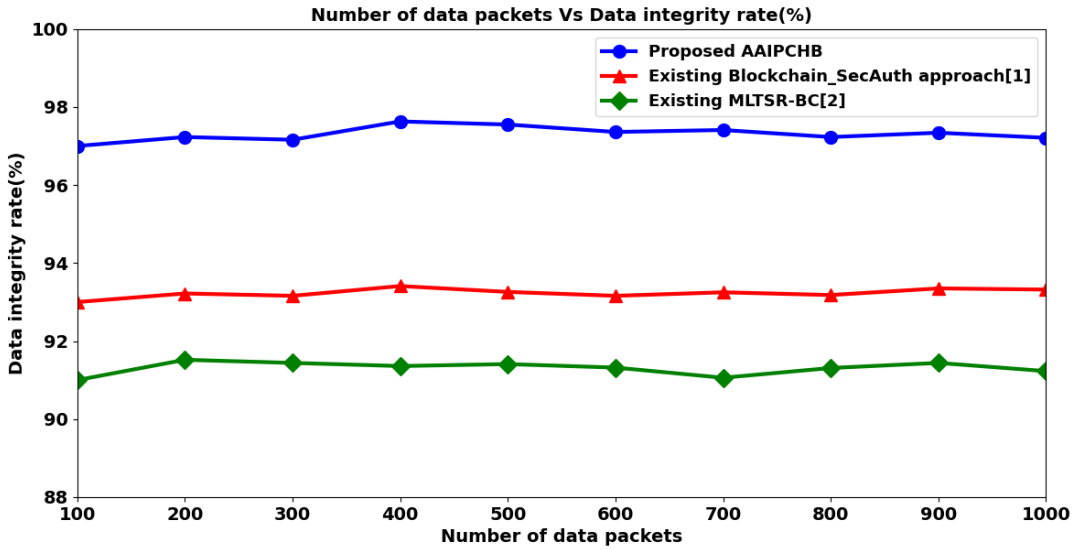

Figure 15 Graphical chart of data integrity rate

Figure 15 demonstrates the comparative examination of the integrity rate achieved by the proposed AAIPCHB method, evaluated against two existing techniques namely, Blockchain_SecAuth approach [1] and MLTSR-BC [2]. The evaluation was performed using number of data packets between 100 and 1000, measuring integrity based on the consistency and reliability across varying sizes. The simulation outcomes reveal that the AAIPCHB method consistently delivers better integrity performance compared to the other two existing methods. For example, with an input of 100 data packets, the AAIPCHB method achieved an integrity rate of 97%, while methods [1] and [2] attained 93% and 91%, respectively. This performance gain remained reliable across all data packets. The average value of ten results specifies that the AAIPCHB method achieved a 4% improvement compared to [1] and a 7% improvement compared to [2] in terms of data integrity rate. This improvement is attained owing to the Davies–Meyer Compression to generate the hash value for each data packets in blockchain construction. The proposed blockchain system, Obershelp pattern recognition technique is integrated into the verification stage to further ensures that the data packets remains unaltered and trustworthy, thereby preserving its integrity.

5.2.4 Packet delivery ratio

This section presents a comparative evaluation of the data confidentiality rate of the proposed AAIPCHB method against existing methods, including the Blockchain_SecAuth approach [1] and MLTSR-BC [2], under varying data packets.

Table 5 comparison analysis of Packet delivery ratio

Number of data packets	Packet delivery ratio (%)		
	Proposed AAIPCHB	Existing Blockchain_SecAuth approach [1]	Existing MLTSR-BC [2]
100	98	95	93
200	98.68	95.32	93.65
300	99.01	95.22	93.05
400	98.89	95.18	93.41
500	98.78	95.62	93.66
600	98.68	95.45	93.45
700	98.82	95.36	93.55
800	98.67	95.36	93.23
900	98.45	95.28	93.41
1000	98.65	95.47	93.35

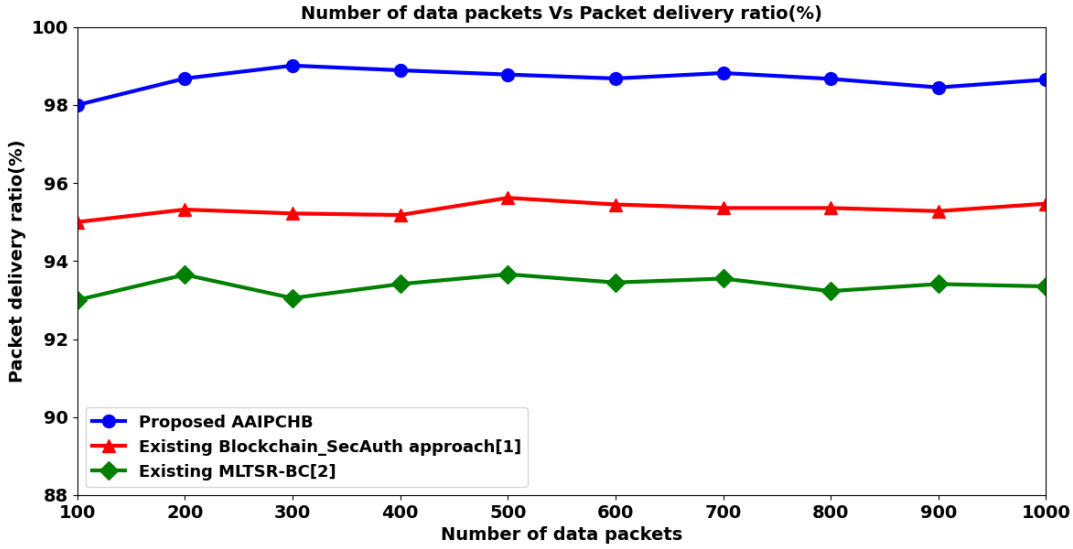

Figure 16 Graphical chart of packet delivery ratio

Figure 16 illustrates the performance analysis of packet delivery ratio using three different methods namely the proposed AAIPCHB method, Blockchain_SecAuth approach [1] and MLTSR-BC [2]. In the graphical chart, the x-axis represents the number of data packets, ranging from 100 to 1000, while the y-axis demonstrates the corresponding packet delivery ratio. Among all the three methods, AAIPCHB method consistently achieved superior performance in packet delivery ratio. For example, when 100 data packets are considered, the AAIPCHB method records an average packet delivery ratio of 98%, whereas [1], [2] achieved packet delivery ratio of 95%, and 93%, respectively. This evaluation was conducted across ten varied data packets volumes, and the results reveal an obvious development. The AAIPCHB

method maintains higher packet delivery ratio rate in all cases. The average of ten results designates that the AAIPCHB method outperforms the existing techniques by approximately 4% compared to [1], 6% compared to [2]. The improved performance of AAIPCHB method is achieved due to the incorporation of a Agentic AI to discover the normal or intruder nodes with higher accuracy. The normal node performs the data aggregation process for transferring the data packets to the sink node for efficient data transmission. As a result, the AAIPCHB method considerably increases the reliability of data transmission from source to sink in WSN.

5.2.5 Data Aggregation delay

This section presents a comparative evaluation of the data confidentiality rate of the proposed AAIPCHB method against existing approaches, including the Blockchain_SecAuth method [1] and MLTSR-BC [2], under varying traffic loads.

Table 6 comparison analysis of data aggregation delay

Number of data packets	Data Aggregation delay (ms)		
	Proposed AAIPCHB	Existing Blockchain_SecAuth approach [1]	Existing MLTSR-BC [2]
100	10.8	12.5	14.8
200	11.2	14.3	16.5
300	12.8	15.5	18.3
400	13.2	16.2	20.4
500	14.8	17.4	22.3
600	15.7	18.2	23.5
700	17.2	20.4	25.4
800	20.4	23.3	28.7
900	21.8	25.7	30.2
1000	25.4	28.2	33.6

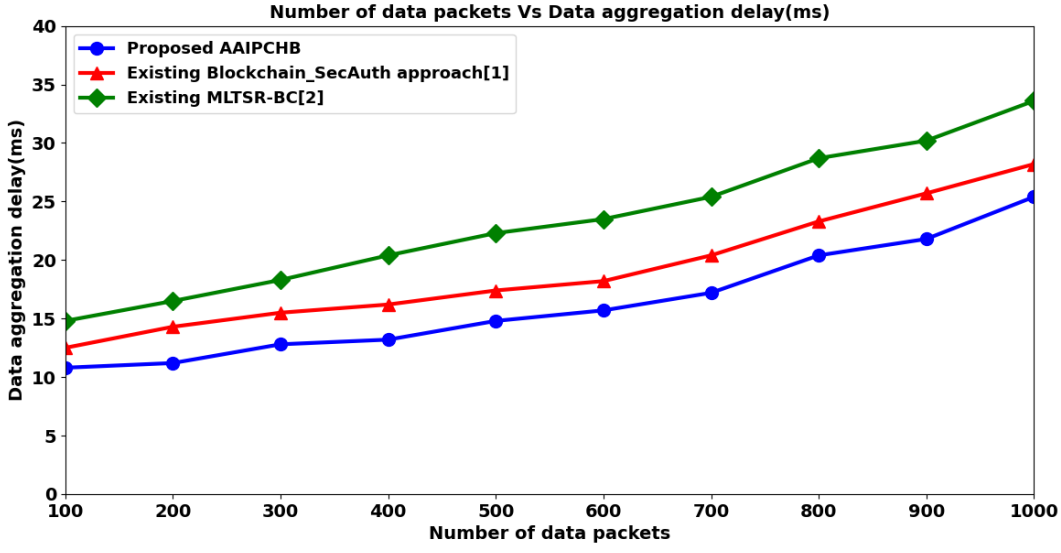

Figure 17 Graphical chart of data aggregation delay

Figure 17 illustrates a performance evaluation of data aggregation delay versus number of data packets ranges from 100 to 1000. The results expose that data aggregation delay of all three methods gets increased while increasing the data packet amounts. However, AAIPCHB method consistently demonstrates an important reduction in data aggregation delay compared to the conventional deep learning approaches Blockchain_SecAuth approach [1] and MLTSR-BC [2]. For instance, when 100 data packets are considered in first iteration, the AAIPCHB method records a delay of 10.8ms, while the existing methods in [1] and [2] demonstrate the performance outcomes observed to be 12.5 ms and 14.8 ms, respectively. Across increasing data volumes, the AAIPCHB method achieves an average delay reduction of approximately 15% and 30% compared to the existing techniques. This improvement is primarily attributed to the integration of the agentic AI model, which selects normal sensor nodes based on such as energy consumption, trust, and signal strength. By classifying and most normal sensor nodes, the system enables faster data aggregation with minimal delay.

5.2.6 Throughput

This section provides a comparative analysis of the throughput achieved by the proposed AAIPCHB method in comparison with existing approaches, namely the Blockchain_SecAuth method [1] and MLTSR-BC [2], across different size of data packets.

Table 7 comparison analysis of Throughput

Size of Data packet (KB)	**Throughput(bps)**		
	Proposed AAIPCHB	**Existing Blockchain_SecAuth method [1]**	**Existing** MLTSR-BC [2]
100	265	215	180
200	372	268	215
300	522	364	310
400	635	477	422
500	766	623	536
600	923	711	633
700	1225	963	845
800	1474	1132	1024
900	1685	1365	1258
1000	1932	1652	1487

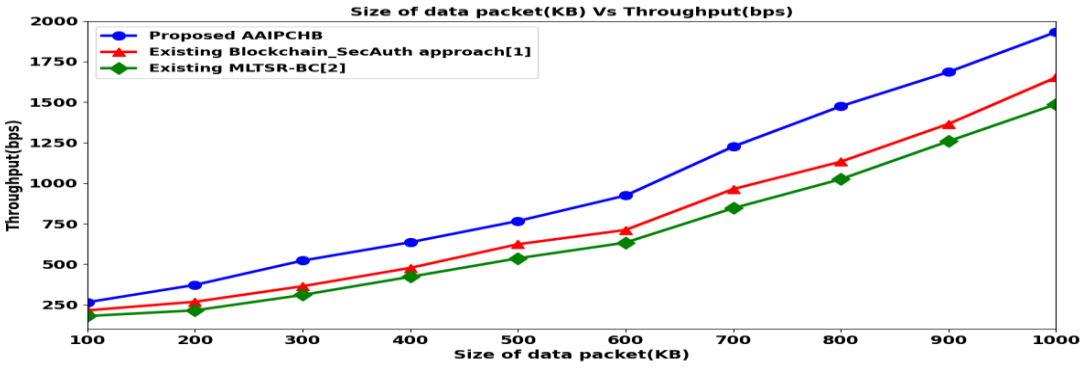

Figure 18 Graphical chart of throughput

Figure 18 shows the graphical assessment of throughput across three different methods namely AAIPCHB method, existing methods, namely Blockchain_SecAuth method [1] and MLTSR-BC [2]. As exposed in graphical figure, the horizontal axis represents the size of data packets being transmitted ranging from 100KB to 1000KB, while the vertical axis demonstrates the performance analysis of throughput. Among the different approaches, AAIPCHB method consistently reveals superior performance, generating a throughput of data packets aggregation successfully. During the initial simulation run, 100 KB of data packets were transmitted from the source node. In this condition, the AAIPCHB method achieved a throughput of 265 bps for successfully delivered data at the sink node. In contrast, methods [1] and [2] achieved throughput values of 215bps and 180bps, respectively. The simulation was conducted over numerous iterations, and the averages of ten results were used for the final performance assessment. The results demonstrate that the AAIPCHB method increases the performance of throughput approximately by 29% and 48%, respectively. This efficient node selection improves data forwarding efficiency and significantly enhances overall network throughput in the WSN environment.

6. Conclusion

This article designs an AAIPCHB method for secure and energy-optimized data aggregation in WSN. The suggested AAIPCHB method begins by deploying numerous sensor nodes throughout a sensor network. An Agentic AI is then employed to categorize these nodes as either normal or intruders based on factors such as residual energy, trust level, and received signal strength. This AI strategy improves overall classification performance. After the classification, the Koorde Cryptographic hash Blockchain is employed to perform the secure aggregation from sensor node to the sink node using Davies–Meyer compression function for preserving the data integrity and confidentiality. The proposed AAIPCHB method is thoroughly estimated through simulations using several performance indicators, including classification accuracy, confidentiality rate, integrity rate, packet delivery ratio, aggregation delay an throughput. Simulation results from the assessment demonstrate that the AAIPCHB method consistently outperforms existing techniques. Notably, it achieves classification accuracy, confidentiality rate, integrity rate, packet delivery ratio while also significantly reducing aggregation delay when compared to traditional methods.

References

1. Sangeetha Yempally , Sanjay Kumar Singh ,Velliangiri Sarveshwaran, “A secure authorization in Multi-WSN based on Blockchain_SecAuth approach for secure data communication”, Blockchain: Research and Applications, Elsevier, 2025 ,Pages 1-22. https://doi.org/10.1016/j.bcra.2025.100331
2. S. Ramachandra, M. Baskar, “Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain” Results in Engineering, Elsevier, Volume 26, June 2025,Pages 1-10. https://doi.org/10.1016/j.rineng.2025.104732
3. Saravanakumar Pichumani, T. V. P. Sundararajan & S. M. Ramesh, “Federated stochastic gradient averaging ring homomorphism based learning for secure data aggregation in WSN”, Scientific Reports, Volume 15, 2025, Pages 1-20. https://doi.org/10.1038/s41598-025-03257-4

4. Meshari D. Alanazi, "A triple-layer authentication framework with elliptic curve cryptography for securing IoT-assisted wireless sensor networks", PLoS One, Volume 20, Issue 8, Pages 1-27. https://doi.org/10.1371/journal.pone.0329011
5. Yichao Taoa , Chenggui Wangb , Huanlong Qin, "Research on Feistel Encryption Algorithm Based On Wireless Medical Sensor Networks", Procedia Computer Science, Elsevier, Volume 259, 2025, Pages 888-896. https://doi.org/10.1016/j.procs.2025.04.041
6. Jing Xiao, Chaoqun Li, Zhigang Li & Jie Zhou, "BS-SCRM: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques", Scientific Reports volume 14, 2024, Pages 1-14. https://doi.org/10.1038/s41598-024-60338-6
7. Marwa E. Madkour, Salah E. Soliman, Moawad I. Dessouky, Fathi E. Abd El-Samie, Mohammed E. Hammad & Amir S. Elsafrawey, "Compressive sensing techniques based on secure data aggregation in WSNs", Scientific Reports, volume 15, 2025, Pages 1-15. https://doi.org/10.1038/s41598-025-14959-0
8. Mohsen Zarei, Mohammad Hosein Fatehi Dindarlou, Mehdi Taghizadeh & Jasem Jamali, "Enhancing the LEACH protocol and lightweight chaotic cryptography for secure data transmission in wireless sensor networks", Scientific Reports volume 15, 2025, Pages 1-26. https://doi.org/10.1038/s41598-025-26370-w
9. Vincent Omollo Nyangaresi, Ganesh Keshaorao Yenurkar, "Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks", High-Confidence Computing, Elsevier, Volume 4, Issue 20, 2024, Pages 1-14. https://doi.org/10.1016/j.hcc.2023.100178
10. M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya & H. Abdul Gaffar, "Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks", Scientific Reports, volume 15, 2025, Pages 1-18. https://doi.org/10.1038/s41598-025-03558-8
11. Sreeja Balachandran Nair Premakumari, Gopikrishnan Sundaram, Marco River, Patrick Wheeler and Ricardo E. Pérez Guzmán, "Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks", Sensors, Volume 25, Issue 7, 2025, Pages 1-13. https://doi.org/10.3390/s25072056
12. Hamad Aldawsari, "A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities", Alexandria Engineering Journal, Elsevier, Volume 126, July 2025, Pages 1-7. https://doi.org/10.1016/j.aej.2025.04.052
13. Kai Guo, Chengyuan Zhan, Muqing Niu, Xiang Li, Zeyu Zheng & Ashutosh Sharma, "An integrated IoT and blockchain lightweight framework for secure smart cities", Discover Internet of Things, Springer, Volume 6, 2026, Pages 1-27. https://doi.org/10.1007/s43926-025-00273-8
14. Rida Batool, Nargis Bibi, Samah Alhazmi and Nazeer Muhammad, "Secure Cooperative Routing in Wireless Sensor Networks", Applied Sciences, Volume 14, Issue 12, 2024, Pages 1-15. https://doi.org/10.3390/app14125220
15. Chindiyababy Uthayakumar, Ramkumar Jayaraman, Hadi A. Raja and Noman Shabbir, "QSEER-Quantum-Enhanced Secure and Energy-Efficient Routing Protocol for Wireless Sensor Networks (WSNs)", Sensors, Volume 25, Issue 18, 2025, Pages 1-20. https://doi.org/10.3390/s25185924
16. Seyed Salar Sefati, Seyedeh Tina Sefati, Saqib Nazir, Roya Zareh Farkhady and Serban Georgica Obreja, "Federated Reinforcement Learning with Hybrid Optimization for Secure and Reliable Data

Transmission in Wireless Sensor Networks (WSNs)", Mathematics, Volume 13, Issue 19, 2025, Pages 1-37. https://doi.org/10.3390/math13193196

17. Sumaira Bashir and Amit Sharma, "Developing A Lightweight Homomorphic Encryption Technique for Secure Data Transmission", CyberSystem Journal, Volume 2, Issue 2, 2025, Pages 98-105. https://doi.org/10.57238/csj.2025.1018
18. Bhanu Priyanka Valluri, Nitin Sharma, "Exceptional key based node validation for secure data transmission using asymmetric cryptography in wireless sensor networks", Measurement: Sensors, Elsevier, Volume 33, 2024, Pages 1-11. https://doi.org/10.1016/j.measen.2024.101150
19. Burhan Ul Islam Khan, Khang Wen Goh, Abdul Raouf Khan, Megat F. Zuhairi , and Mesith Chaimanee, "Resource Management and Secure Data Exchange for Mobile Sensors Using Ethereum Blockchain", Symmetry, Volume 17, Issue 1, 2025, Pages 1-31. https://doi.org/10.3390/sym17010061
20. Osama A. Khashan, Nour M. Khafajah, Waleed Alomoush, Mohammad Alshinwan, "Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks", IEEE Access, Volume 12, 2024, Pages 23290 – 23304. **DOI:** 10.1109/ACCESS.2024.3360488
21. Pooja Anand, Yashwant Singh & Harvinder Singh, "Secure IoT data dissemination with blockchain and transfer learning techniques", Scientific Reports, volume 15, 2025, Pages 1-29. https://doi.org/10.1038/s41598-024-84837-8
22. Samuel Kofi Erskine, "Secure Data Aggregation Using Authentication and Authorization for Privacy Preservation in Wireless Sensor Networks", Sensors, Volume 24, Issue 7, 2024, Pages 1-27. https://doi.org/10.3390/s24072090
23. [23] Muzammil Hussain, Mudassar Hussain, Najmuddin Aamer & Farhan Shaikh, "Optimized rank-based key management for energy-efficient routing in wireless sensor networks for IoT applications", Discover Internet of Things, Springer, Volume 5, 2025, Pages 1-31. https://doi.org/10.1007/s43926-025-00224-3
24. [24] Osama A. Khashan, "Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks", Knowledge-Based Systems, Elsevier, Volume 304, 2024, Pages 1-36. Https://doi.org/10.1016/j.knosys.2024.112557
25. [25]NasirAyub,SalheenBakhet,Muhammad Junaid Arshad, Muhammad Usman Saleem ,Dr.Rimsha Anam ,Muhammad Zubair Fuzail, "An Enhanced Machine Learning And Blockchain-Based Framework For Secure And Decentralized Artificial Intelligence Applications In 6g Networks Using Artificial Neural Networks (ANNS)", Spectrum of Engineering Sciences, Volume 3, Issue 4, 2025, Pages 348–364. https://thesesjournal.com/index.php/1/article/view/261
26. [26] Bharat Kumara, S. Anantha Padmanabhan, "A condition-based distributed approach for secured privacy preservation of nodes in wireless sensor networks IoT", International Journal of Reconfigurable and Embedded Systems, Volume 13, Issue 2, 2024, Pages 441-449. DOI:10.11591/ijres.v13.i2.pp441-449
27. [27] Ponnusamy Chinnasamy, G. Charles Babu, Ramesh Kumar Ayyasamy, S. Amutha, Keshav Sinha and Allam Balaram, "Blockchain 6G-Based Wireless Network Security Management with Optimization Using Machine Learning Techniques", Sensors, Volume 24, Issue 18, 2024, Pages 1-19. https://doi.org/10.3390/s24186143
28. [28] dil O. Khadidos, Nawaf Alhebaishi, Alaa O. Khadidos, Mohammed Altwijri, Ayman G. Fayoumi, Mahmoud Ragab, "Efficient key distribution for secure and energy-optimized

communication in wireless sensor network using bioinspired algorithms", Alexandria Engineering Journal, Elsevier, Volume 92, April 2024, Pages 63-73. https://doi.org/10.1016/j.aej.2024.02.064

29. Umar Draz, Tariq Ali, Sana Yasin, Mohammad Hijji, Muhammad Ayaz and EL-Hadi M. Aggoune, "Decentralized Energy Swapping for Sustainable Wireless Sensor Networks Using Blockchain Technology", Mathematics, Volume 13, Issue 3, 2024, Pages 1-32. https://doi.org/10.3390/math13030395 .