International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing Vehicular Internet of Things (V-IoT) Communication in Smart VANET Infrastructure using Multi-layered Communication Framework and Novel Threat Detection Algorithm

Pratima Upadhyay [1], Samta Jain Goyal [2], Venkatadri Marriboyina [3], Sunil Kumar[4,5]

Submitted: 25/09/2023 **Revised**: 17/11/2023 **Accepted**: 27/11/2023

Abstract: In latest technological paradigm, the incorporation of Vehicular Ad-Hoc Networks (VANETs) architecture with the Internet of Things (IoT) devices in smart transportation systems has introduced new proportions to reliable data communication. However, ensuring secured dynamic addition of IoT nodes and mitigating probable threats like Denial of Service (DoS) attacks, eavesdropping and malware poses a serious challenge in ensuring an efficient communication links. The VANET-IoT (V-IoT) system offers increased addition of IoT devices and its associated scalability but the increasing device usage to maintain low-latent connectivity poses serious threat and highly exposes the infrastructure to attacks. The need for secured node authentication in V-IoT is hence found essential to ease the deployment of new sensing devices without compromising on security. Conventional methods fails to offer a holistic approach in V-IoT system that combines authentication and threat detection via edge computing to ensure the communication reliability and security in V-IoT system. This research proposes a novel multi-layered V-IoT smart infrastructure with various components including authentication, IoT device integration, edge computing, and intelligent threat classification to maintain secured and efficient communication. An Evolutionary Multimodal Optimization (EMO) based Probabilistic Adversarial Ada-Transform (PAAT), a cutting-edge algorithm act as an authenticator and threat classifier in identifying DoS attacks, malware, and eavesdropping attempts in V-IoT systems. This multi-layered framework enables edge computing technology to append EMO-PAAT on V-IoT system for authentication and threat detection. Various parameters including scalability; algorithm performance; and V-IoT performance is measured via different metrics like Processing Time, Throughput, CPU and Memory Utilization, Latency; Detection Rate; and Communication Overhead, and Energy Consumption, respectively are utilized to evaluate the performance. Thus, significant improvements are reported in V-IoT system to maintain a secured and reliable communication.

Keywords: *Security, V-IoT, VANETs, Threat Detection, Edge Computing, Authentication*

1. Introduction

The Internet of Things (IoT) in Vehicular Ad-Hoc Networks (VANETs) [1] have recently merged to create a new paradigm called as the Vehicular Internet of Things (V-IoT) [2]. V-IoT offers a real-time intra-data transmission between vehicles, smart devices and infrastructure, which potentially transforms the Intelligent Transportation System (ITS) [3, 4]. However, the integration of IoT in V-IoT with inter-communication introduces novel difficulties for VANETs in terms of data security, scalability, and efficiency [5].

VANETs are a self-organizing, dynamic network in which moving vehicles exchange data between each another and with fixed Road Side Unit (RSU) [5,6]. The emerging ITS rely on VANETs to ease essential services like emergency response, traffic management, and vehicle-to-vehicle (V2V) communication [7]. Further, incorporating IoT devices into VANETs improves the functionality of useful data collection and transmission from a wide range of sensors, thereby ensuring secure and effective transportation [8].

Unique challenges arise while adding IoT devices in VANETs include dynamic addition of IoT, resource consumption and network being prone to various threats [9] like Denial of Service (DoS) attacks, eavesdropping and malware infiltrations [10]. To overcome such challenges, V-IoT needs an encompassing strategy for a secured and streamlined connectivity. The current research and systems on V-IoT are vulnerable to these attacks/threats and the increasing resource consumption poses security risk that compromises the overall performance. The need for securing the IoT devices against these security attacks requires a secured multi-layered node authentication process to safeguard the V-IoT and to reduce the computational time and processing for sensing IoT device addition. A robust solution is

[1] *Research Scholar, Department of Computer Science & Engineering, Amity School of Engineering and Technology, Amity University, Gwalior. Madhya-Pradesh, India. (pratimaupadhyay784@gmail.com)*

[2] *Associate Professor, Dept. of CSE, ASET, Amity University, Gwalior (M.P.) India. (sjgoyal@gwa.amity.edu)*

[3] *Principal and Professor in CSE at NITTE Institute of Professional Education, Mangalore India. (venkatadri.mr@gmail.com)*

[4] *Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*

[5] *Department of Computer Science, Graphic Era Hill University, Dehradun 248001, India (drskumar.cs@gmail.com)*

needed as both the objectives creates a trade-off between them to maintain security and efficiency.

This research aims to develop a smart multi-layered V-IoT infrastructure that encompasses edge computing mechanism to enable IoT device authentication and intelligent threat classification. The smart multi-layered V-IoT edge infrastructure identifies and characterize various security threats including DoS attacks, eavesdropping attempts, and malware incursions. A suitable authentication and security threat detection algorithm is developed using Evolutionary Multimodal Optimization (EMO) and Probabilistic Adversarial Ada-Transform (PAAT) techniques to improve the accuracy and efficiency in identifying security threats.

In this paper, a holistic smart multi-layered V-IoT Edge integrates diverse IoT devices, edge computation, and intelligent threat classification. The development of EMO-PAAT algorithm enables precise authentication and efficient security threat detection.

The main contribution of the research involves addressing the related to security and efficiency enhancement in V-IoT data communication.

- The authors develop a Multi-Layered V-IoT Edge Infrastructure with diverse IoT devices, which employs a new Vehicular Constrained Application Protocol (V-CoAP) protocol with auto-configuration for seamless connectivity.
- The authors use edge computing to authenticate the new IoT nodes in Multi-Layered V-IoT Edge Infrastructure. The authentication provides insights from the generated IoT data prior transmission to the Centralized Servers (CS) or Software-Defined Networking (SDN)/Storage Controllers (SC) via edge controllers. This authentication process enhances the security by authorizing malignant devices to participate in data exchange process. The Multi-Layered V-IoT Edge Infrastructure ensures a high-bandwidth and low-latency communication channels in V-IoT, which is crucial for supporting the data transmission from IoT devices to CS or SDN/SC.
- The authors develop a new AI-based authentication and threat classification algorithm in edge system to monitor the V-IoT infrastructure that facilitates authentication via EMO and threat classification via PAAT against DoS, malware, and eavesdropping in V-IoT environment.

The outline of the paper involves the following: section 2 discusses the related works. Section 3 elaborates the proposed Multi-Layered V-IoT Edge Infrastructure with authentication and security threat classification. Section 4 evaluates the entire infrastructure over wide range of performance metrics. Section 5 concludes the work with directions for future scope.

2. Related Works

In this section, various VANETs and integrated V-IoT systems are presented, which addresses the critical issues such as privacy, security, scalability, and communication efficiency. These techniques offer insights into the ITS landscape concerning only the vehicular communication and offers improved solutions to enhance the security and performance of these networks.

1. Security Schemes in VANET-IoT

In VANETs, the combined security and privacy modelling in [11] introduces a provision to seamless IoT services via blockchain security framework (BSF) while preserving the user privacy in 5G-enabled infrastructure. The BSF-5G infrastructure offers real-time trust management in vehicular message exchange, video reporting with acceptable network overhead. Clustering and Trust modelling in [12] improves the security and stability in VANETs by mitigating the power consumption and bandwidth issues. The trust-based clustering groups with limited nodes and the reputation, knowledge and experience components selects the trustworthy CHs to find the malignant nodes. Thus, reduction in computational overhead is achieved with possible identification of malicious vehicles and security against attacks. 6G Communications in [13] integrates 6G communications with VANETs to control the traffic and ensures security.

Information-Centric Networking (ICN) in [14] explores multiple strategies to improve the security and performance-related message dissemination. It overcomes traditional IP-based networking and introduces an ICN proactive caching called Left-Right-Front to strategically optimizes the VANETs by placing the content at appropriate nodes. The timely messages dissemination outperform other caching methods in terms of utilization, and enhanced VANET efficiency. The Edge Computing technology in [15] develops a model to integrate the blockchain and edge computing to improve security and reduce communication delays in VANETs. This QoS aware Software-defined Network (SDN) in VANETs with Edge Computing enhances the performance with reduced delays, secure delivery and improved message reliability. The heuristic algorithms address the security and message failures with 55% reduction in delay, and improved reliability.

Formal Modeling in [16] represent an IoT-based vehicle-life integration for a smart transportation. It uses graph theory, UML, and VDM-SL to ensure the safety and accuracy of ITS with fault detection and it promotes efficient emergency response. The Volunteer Computing in [17] introduces an architecture for satisfying the computational requirements and addresses the need for distributed computing environment. The ridge regression and support vector regression (RR-SVR) achieves reduced error rate on computationally intensive tasks in VANET-IoTs.

2. Authentication Schemes in VANET infrastructure

The authentication scheme in VANET communications in [18] operated on the certificateless aggregate signature (CAS) basis to enhance the security and efficiency. The CAS address the key escrow and certificate management and the individual signature aggregation eliminates pairing operations, which offers enhanced security and efficiency. Thereby, the performance of VANET communication is improved with enhanced security and computational efficiency. In heterogeneous IoT networks, the XGBoost employing in leveraged in [19] is applied on an intrusion detection system over realistic dataset (ToN-IoT) in VANETs. The Identity-Based Encryption (IBE) proposed in [20] enables access control, and when it is combined with deep learning (DL) method it leverages malicious packet detection. With rapid vehicle proliferation, the security concerns and authentication is achieved with 99.72% accuracy in detecting the malicious packets. Blockchain-assisted certificateless key agreement protocol (Block-CLAP) in [21] secures IoV in smart transportation infrastructure. The authentication ensures secured transmission with key management on traffic-centered data and secured data collection at the servers. A low computational and communication overhead is hence achieved after the mitigation of security threats in IoV infrastructure.

While these techniques offer valuable contributions in VANETs, there exist some challenges and that needs to be addressed: initially, many studies focus on specific aspects of VANETs and IoT, i.e. security or communication protocols. However, a comprehensive framework that combines both the elements are not addressed. Secondly, achieving a balance between security and communication efficiency remains a challenge and few methods emphasize security but fails to identify the network performance, and vice versa. Thirdly, with increasing IoT devices in VANETs, scalability tends to be pressing issue and the ability on handling the increasing load and maintaining its network performance is still a bottleneck.

Table 1: Comparison of various state-of-art techniques

Ref	VANET Integration	Problem and Challenges	Techniques Adopted	Novelty	Results achieved
[11]	5G-, SDN, Blockchain	Security and privacy in VANET	Blockchain-based security framework, SDN	Decentralized and immutable blockchain, SDN-enabled 5G-VANET	Malicious node/message detection, Acceptable network performance (95% detection rate)
[12]	Clustering	Clustering stability, security	Trust-based clustering mechanism	Trust-based clustering, Malicious node identification	Increased CH lifetime (40% increase), Reduced computation overhead (25% reduction)
[13]	IoT, AI, Cloud	Traffic control, public safety	Cloud-based database, special traffic rules	Cloud-based traffic control, Real-time warnings	Enhanced public safety, Traffic control (15% reduction in accidents)
[14]	ICN, -IoT	Information sharing in VANETs	ICN-based proactive LRF caching strategy	Proactive caching, Safety message dissemination	Improved cache utilization (25% increase), Better hop ratios (15% improvement)
[15]	SDN, Edge Computing, Blockchain	Communication delay, fault tolerance, security	SDN Fault Tolerance and QoS-Aware IoT-Based VANET	Edge computing, Fault tolerance	Reduced communication delay (55% reduction), Improved fault

					tolerance (30% fewer failures)
[16]	IoT	Vehicle-life integration, emergency communication	UML, graph theory, VDM-SL formal technique	Formal modeling, Emergency communication	Improved emergency communication (20% faster), Formal system modeling
[17]	Volunteer Computing, ML	Computational resource utilization	ML, regression techniques	Volunteer vehicle prediction	Efficient prediction of volunteer vehicle capabilities (>90% accuracy)
[18]	IoT	Authentication, privacy, limited bandwidth, mobility	CAS Authentication Scheme	Aggregate signatures, Reduction in computation overhead	Enhanced security (20% improvement in security), Reduced computation overhead (30% reduction)
[19]	ML	Security against attacks	Machine learning for IDS, ToN-IoT dataset	Realistic dataset, ML-based intrusion detection	Enhanced security (30% higher accuracy)
[20]	6G	Authentication, security	(IBE) - Deep Learning	IND-sID-CCA security, Deep learning detection	Accurate cyber attack detection (99.72% accuracy)
[21]	IoV, Blockchain	Security in IoV	Block-CLAP	Blockchain-based security, Consensus algorithm	Superior security, Low overheads, High consensus rate (98%)

3. Proposed Multi-Layered Smart V-Iot Infrastructure

The proposed method combines IoT device for data collection, edge computing for authentication, and AI-algorithms for advanced threat detection. It leverages AI based EMO-PAAT algorithm to enhance authentication and security. The architectural illustration of proposed Multi-Layered Smart V-IoT Infrastructure is given in Figure 1.

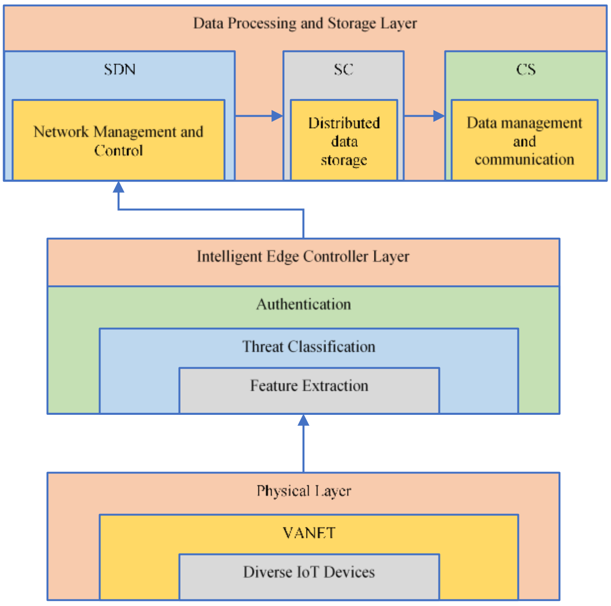

Data Processing and Storage Layer
SDN
Network Management and Control
SC
Distributed data storage
CS
Data management and communication
Intelligent Edge Controller Layer
Authentication
Threat Classification
Feature Extraction
Physical Layer
VANET
Diverse IoT Devices

Fig 1: Multi-Layered Smart V-IoT Infrastructure

1. System Model - IoT in VANET

The proposed method integrates different IoT device configuration into the VANET configuration. This accounts for the diversity of IoT devices and embedding V-CoAP protocols with auto-configuration ability for seamless communication and connectivity. This involves amending IoT device diversity, adopting VANET configuration, modelling V-CoAP in V-IoT and ensuring seamless connectivity.

a) Device Diversity (D):

The diversity (*D*) of IoT devices is embedded within vehicles units or roadside units and it includes communication protocol (V-CoAP), sensor types, and its communication capabilities, and it is defined in Eq.(1)

$$D = \sum_{i=1}^{N_i} N_i \cdot C_{ij} \qquad (1)$$

N_t represents the number of different sensor types.

N_i represents the number of instances of each sensor type.

C_{ij} represents the communication capability of IoT sensor type *i* on index *j*, and

$j \in [1\text{-}3]$ represents the index of *i* ranging between low, medium and high capability.

b) VANET Configuration (VC):

The VC (Eq.(2)) includes the parameters for a vehicle/RSU to establish/maintain connectivity using various factors like transmission power, communication range and network topology.

$$VC = \sum_{i=1}^{N} P_i \cdot R_i \quad (2)$$

where:

N is the number of parameters/settings in the configuration.

P_i represents the i^{th} parameter or setting (i.e. communication range, transmission power).

R_i represents the value or range associated with the (i^{th} parameter.

c) V-CoAP Modelling:

V-CoAP is proposed in this research as a lightweight communication protocol to establish connectivity among the IoT devices and with constrained VANETs environments. It involves the process of IoT device configuration to establish communication using V-CoAP as in Eq.(3).

$$I = \sum_{i=1}^{N} C_i \cdot S_i \qquad (3)$$

where:

I - CoAP Configuration.

N - number of parameters/settings in the V-CoAP configuration.

C_i - i^{th} CoAP parameter.

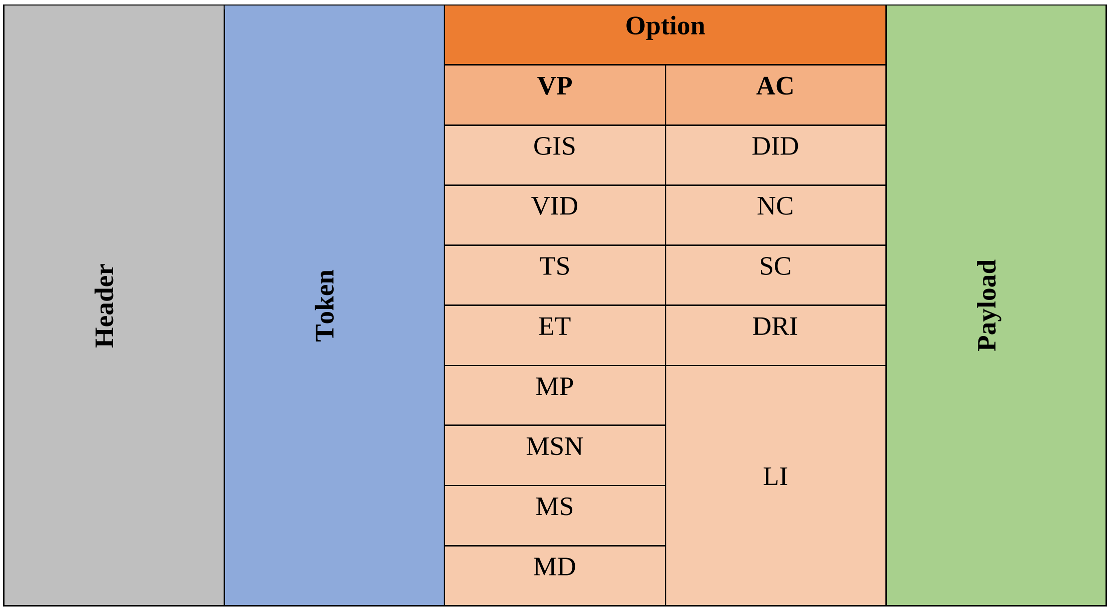
S_i - value or range associated with the i^{th} V-CoAP parameter.

In the proposed V-CoAP, CoAP messages includes different VANET parameters (VP) of V-IoT to establish communication between diverse IoT, vehicles and V-IoT infrastructure. The parameters/ options in CoAP messages involves the following:

The Header contains the control information like message type (Confirmable/Non-confirmable), message code (GET/POST), and message ID for message handling and identification. Token is used for correlation and message identification between requests and responses. A set of options provides parameters like VANET specific (Geographic Information (GI), Speed (S), Vehicle ID (VID), Timestamp (TS), Event Type (ET), Message Priority (MP), Message Sequence Number (MSN), Message Signature (MS) and Message Destination (MD)) and auto-configuration parameters (Device ID (DID), Network Configuration (NC), Security Configuration (SC), Data Reporting Interval (DRI) and Location Information (LI)) related to the message that includes URI path, content format, or observe options. Auto-configuration (AC) mechanisms enable the IoT devices to discover/configure automatically the network settings and it is crucial for IoTs to adapt with dynamic network conditions. The parameters required to autoconfigure the IoTs is defined in Eq.(4):

$$AC = \{X_1, X_2, \ldots, X_5\} \qquad (4)$$

As in Figure 2, the research uses five different auto-configuration parameters including Device ID (X_1), Network Configuration (X_2), Security Configuration (X_3), Data Reporting Interval (X_4) and Location Information (X_5). Finally, the payload carries application-specific data relevant to the V-CoAP request or response.



Header	Token	Option		Payload
		VP	AC	
		GIS	DID	
		VID	NC	
		TS	SC	
		ET	DRI	
		MP	LI	
		MSN		
		MS		
		MD		

Fig 2: Representation of Proposed V-CoAP message for V-IoT with VANET parameters

Finally, seamless communication is ensured among all the devices in the multi-layered V-IoT infrastructure.

2. Edge Computing Process

Edge computing is utilized to perform feature extraction-based authentication on IoT nodes using EMO. This step extracts valuable features from the data generated by IoT devices using EMO before transmitting it to CS or SDN/SC. The extracted features are verified to authenticate the nodes for the transmission of collected data and this enhances security by ensuring that only authorized devices can participate in data exchange.

The process involves the collection of the generated data (d), and EMO is used for the extraction of the valuable features. The PAAT authentication mechanism uses extracted features for authenticating IoT nodes, where the extracted features of the authorized IoT device profile are compared to find if the IoT nodes are authorized or not. Finally, the decision is made based on the authenticated result and upon successful authentication of node, the data transmission is initiated and vice versa.

a) EMO Feature Extraction

The Feature Extraction (FE) process uses EMO to optimizing the valuable feature extraction from the diverse IoT device data. EMO finds the optimal features set, which is required to authenticate the IoT nodes in V-IoT infrastructure. This involves the following process as in Figure 3.

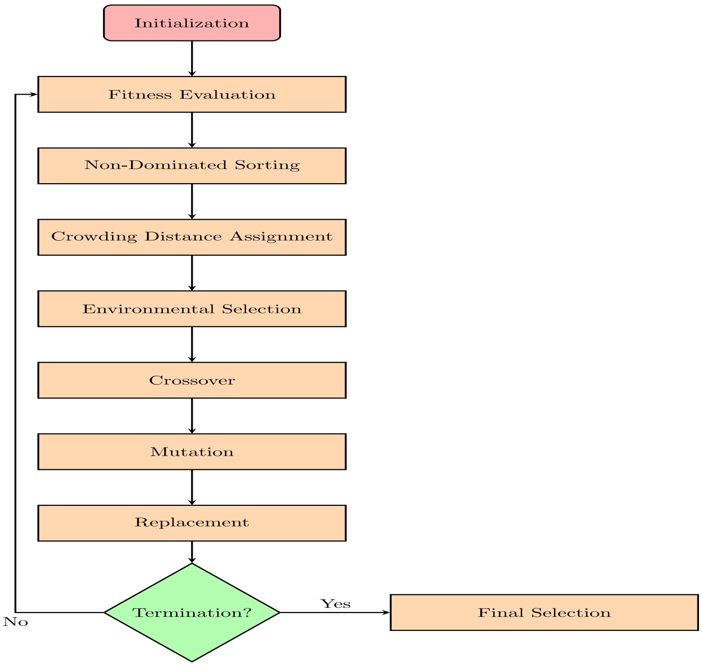


Fig 3: EMO Process Flow

Initialization:

The EMO initializes the population of feature sets, which is the viable candidate solution. The candidate vector set of a specific IoT feature is represented in Eq.(5):

$$f\{x\} = [x_1, x_2, x_3, \ldots, x_n] \quad (5)$$

Where:

$f\{x\}$ - feature set vector, and

x_i - extracted attribute from the data.

Fitness Evaluation:

The quality of feature set is evaluated using a fitness function, which measures the accurate representation of features present in a set corresponding to the original data. This function serves the authentication mechanism as it finds the accurate feature required for the process of diverse IoT node authentication. Mathematically, the optimization problem for the authentication using a dataset features x is represented in Eq.():

$$\text{Maximize } f(x) \text{ s.t. } f(x) \rightarrow \Omega \quad (6)$$

Where:

$f(x)$ - fitness function to evaluates the feature set quality.

Ω - feasible solution space.

EMO finds the feature set $f(x)^*$ to maximizes the fitness in the solution space and this process is iterative until a convergence is attained to find an optimal solution.

Consider D as the collected dataset with n IoT devices, where observation is represented as x_i and i being the index of observations. The variable A represents the authorized or legitimate IoT from the feature set. The research uses correlations between the variables (Table 2) and hence it uses Mahalanobis Distance to deal with various data scales (Table 3). The expression for correlation is given in Eq.(7):

$$F(x) = \max_{a \in A} (x-a)^{T} M(x-a) \quad (7)$$

where, M - covariance data vector and a - nearest authorized entity in a set A.

Table 2: Extracted Feature Category from diverse IoT dataset

Feature Category	Features Extracted
Temporal Features	Timestamp, Time of Day, Day of Week
Spatial Features	GPS Coordinates, Location IDs
Sensor Readings	Temperature, Humidity, Light Intensity
Device Information	Device ID, Manufacturer, Firmware Version
Network Information	Signal Strength, Network Latency
Environmental Data	Air Quality Index (AQI), Noise Level
Event Data	Alarm Triggered, Motion Detected
Energy Consumption	Battery Level, Power Usage

Table 3: Feature values extracted from the collected diverse IoT dataset

Sensor Name	Timestamp	Location	Features
Temperature and Humidity Sensor	2023-09-15 08:30:00	Latitude 34.0522, Longitude -118.2437	Temperature: 25.3°C, Humidity: 52%
Smart Light Bulb	2023-09-15 19:45:00	Room 102	Light Intensity: 450 Lux
GPS Tracking Device (Vehicle)	2023-09-15 14:15:00	Location: Latitude 40.7128, Longitude -74.0060	Vehicle ID: XYZ123
Air Quality Monitor	2023-09-15 12:00:00	Outdoors	AQI: 78 (Moderate)
Smart Security Camera	2023-09-15 21:10:00	Front Door	Event: Motion Detected

IoT Gateway Device	2023-09-15 16:30:00	Device ID: IoTGW001	Network Latency: 32 ms
Wearable Health Monitor	2023-09-15 07:00:00	-	Heart Rate: 78 bpm, Blood Pressure: 120/80 mmHg

Crowding Non-Dominated Sorting:

The solutions are categorized into various fronts using non-dominated sorting and the first front solutions, which are non-dominated is regarded as the Pareto-optimal Solution (POS). The crowding distance is estimated for POS front and it measures how well a solution is crowded within its front based on its proximity to other solutions. This solution is applied for the process of selection, where it has a higher crowding distance with the first front.

Selection:

The selection involves picking the candidate feature sets for the next generation using its highest fitness level . The selection probability of an individual *i* is determined using max*F*(*i*). The roulette wheel selection method is used to calculate the selection probability (*P*) as it is directly related with the individual fitness as in Eq.(8):

$$P(i) = \frac{F(i)}{\sum_{j=1}^{N} F(j)} \tag{8}$$

where, *P*(*i*) - individual *i* selection probability, *N* - population size, and *F*(*j*) - fitness of an individual *j*.

Crossover:

The selected feature set pairs undergo the process of crossover to form new candidate sets. Consider two parents *A* and *B* with a random selection of a crossover point *k* and it creates a two new offspring using the swapping process before and after k and it is expressed in Eq.(9) and Eq.(10), respectively:

$$A' = A[1:k] + B[k+1:N] \tag{9}$$

$$B' = B[1:k] + A[k+1:N] \tag{10}$$

where, *A*' and *B*' - offspring, and *N* - chromosome length.

Mutation:

Random modification is made to the features using certain candidate feature sets. Each chromosome is defined as a binary string of length *N* (N - number of genes). The mutation operation applies flipping operation on a randomly chromosome bit with a probability P_m (i.e. mutation rate). Consider a chromosome $C = (c_1, c_2, \ldots, c_N)$, where c_i is the i^{th} chromosome bit and the flipping operation is expressed in Eq.(11):

$$c_i' = \begin{cases} 1 - c_i & if\ P = P_m \\ c_i & if\ P \neq P_m \end{cases} \tag{11}$$

where,

c_i - original bit value at i^{th} position in a chromosome.

c_i' - mutated bit value at i^{th} position in a chromosome.

The new feature sets generation replaces the previous generation and the optimization continues until a convergence criterion is met. The selected feature set using EMO is hence selected as the final set of features.

3. *PAAT Authentication and Decision Making*

The authentication of IoT nodes using PAAT in an edge network involves comparing the transformed IoT feature set with well-known legitimate IoT device profiles. This comparison is used to find the authenticity of the IoT device present in V-IoT system.

Initially, feature set transformation is applied by considering the feature extracted F_d from the data generated by the IoT device, which needs to be authenticated in edge server for possible data transmission and storage to CS or SDN. Secondly, it applies PAAT to F_d as $T(F_d)$, where Adversarial Ada-Transform is used to transform the data, and it uses probabilistic elements to check the authenticity of F_d. The transformed feature set $T(F_d)$ is compared with the trusted IoT device profiles. These profiles $(P_1, P_2, \ldots, P_n)$, where *n* is the total trusted IoT devices.

The similarity or dissimilarity is measured between $T(F_d)$ and the trusted profile P_i using cosine similarity, which is calculated using the following Eq.(12):

$$\mathrm{Cos}(T(F_d) \cdot P_i) = \frac{T(F_d) \cdot P_i}{\left\| T(F_d) \right\| \cdot \left\| P_i \right\|} \tag{12}$$

where, $T(F_d) \cdot P_i$ - dot product between the transformed feature set and the trusted profile, while $\| T(F_d)\|$ and $\|P_i\|$ - magnitudes.

A similarity threshold β is used to measure similarity score (*SS*) between $T(F_d)$ and P_i and upon exceeding the threshold, the IoT node is authenticated. This enables the authentication decision to grant access to connect with V-IoT network.

```
Algorithm 1: PAAT Authentication and Decision Making
# Define trusted profiles or templates for legitimate IoT devices
                    $P_i = [P_1, P_2, \ldots, P_n]$
# Define a similarity threshold for authentication
                    $\beta$ = Similarity threshold
# Compute cosine similarity between two vectors:
                    $\text{Cos}(T(F_d) \cdot P_i) = \frac{T\left(F_d\right) \cdot P_i}{\left\|T\left(F_d\right)\right\| \cdot \left\|P_i\right\|}$
# Authenticate an IoT device
def auth($F_d$):
    # Transform the feature set $F_d$ using the PAAT
                    $T(F_d) = \text{PAAT}(F_d)$
    # Initialize a variable to keep track of the highest similarity score
                    $\max \text{Cos}(T(F_d) \cdot P_i) = 0$
    # Iterate through trusted profiles $P_i$
    for profile in $P_i$:
        # Calculate cosine similarity between the transformed feature set $T(F_d)$ and the profile $P_i$
                    $SS = \text{Cos}(T(F_d) \cdot P_i)$
        # Check if the similarity score $SS$ exceeds the threshold $\beta$
        if $SS > \beta$:
            # If a match is found, grant authentication and exit the loop
            return “Auth”
        # Update the maximum similarity score if needed
        if $SS > \max \text{Cos}(T(F_d) \cdot P_i)$:
                    $\max \text{Cos}(T(F_d) \cdot P_i) = SS$
    # If no match is found among trusted profiles $P_i$, deny authentication
    if $\max \text{Cos}(T(F_d) \cdot P_i) < SS$:
        return “Auth Denied”
```

4. Performance Evaluation

A comprehensive evaluation is conducted in terms of network scalability, algorithm performance and Multi-Layered V-IoT Edge Infrastructure performance between the state-of-art CAS [18], IBE [20] and Block-CLAP [21], and the proposed EMO-PAAT. Further, the algorithm performance is compared with various other XGBoost [19], RR-SVR [17] and Deep Neural Network (DNN) [20]. The proposed Multi-Layered V-IoT Edge Infrastructure ensures the establishment of low-latency and high-bandwidth communication channels within the V-IoT, which is crucial for supporting the transmission of data from IoT devices efficiently.

1. Performance Metrics

Scalability metrics include processing time, throughput, CPU and memory utilization, latency. Multi-Layered V-IoT Edge Infrastructure performance metrics include Communication Overhead and Energy Consumption. The attack detection performance metrics include Detection Rate on DoS attack dataset [22], Malware dataset [23] and eavesdropping dataset [24].

The method includes a comprehensive evaluation process to assess the performance of the proposed framework and the EMO-PAAT algorithm. Various performance parameters are considered:

The scalability determines how well the Multi-Layered V-IoT Edge scales with increased IoT load, and it ensures the ability to handle the increasing IoT devices and data. Similarly, its performance metrics determines the ability and efficiency to perform with increased message and vehicle overload. Finally, the attack detection performance measures the efficacy of these methods to mitigate the DoS, malware, and eavesdropping.

The processing time measure the time to perform the operations in the algorithm and within the framework. Throughput measures the rate at which IoT data is processed and transmitted. CPU and Memory Utilization finds how the resources are efficiently utilized. Latency measures the delay occurring while the IoT data is transmitted. Detection Rate estimates the efficacy of IMO-PAAT in detecting the threats. The communication overhead and energy consumption measure the overhead and total energy, respectively required to authenticate the IoT devices, enable data transmission from V-IoT to edge and then to CS or SDN/SC.

2. Results and Discussion

The experimental setup is presented in Table 4, where the settings are utilized for the purpose of evaluating the efficacy of the proposed method using a simulation tool. NS-2.34 simulation tool is utilized for the purpose of testing the model and this runs on a intel i7 processor with 16GB of RAM.

Table 4: Experimental Setup

Parameter	**Value**
System/Network Model Parameters	
Communication Range (CR)	250 meters
Transmission Power (TP)	20 dBm
Network Topology	Mesh
Network Latency	32 ms
VANET Configuration (VC)	
CR	250 meters
TP	20 dBm
Topology	Mesh
Network Latency	32 ms
EMO Parameters	
Population Size	100
Maximum Generations	50
Crossover Rate	0.8
Mutation Rate	0.1
PAAT Parameters	
Threshold for Authenticity (TA)	0.9
Threshold for Maliciousness (TM)	0.1
Adversarial Transform Rate (ATR)	0.05
Probabilistic Acceptance Rate (PAR)	0.95

Using table 4, the comparison of different metrics is compared and the results are presented.

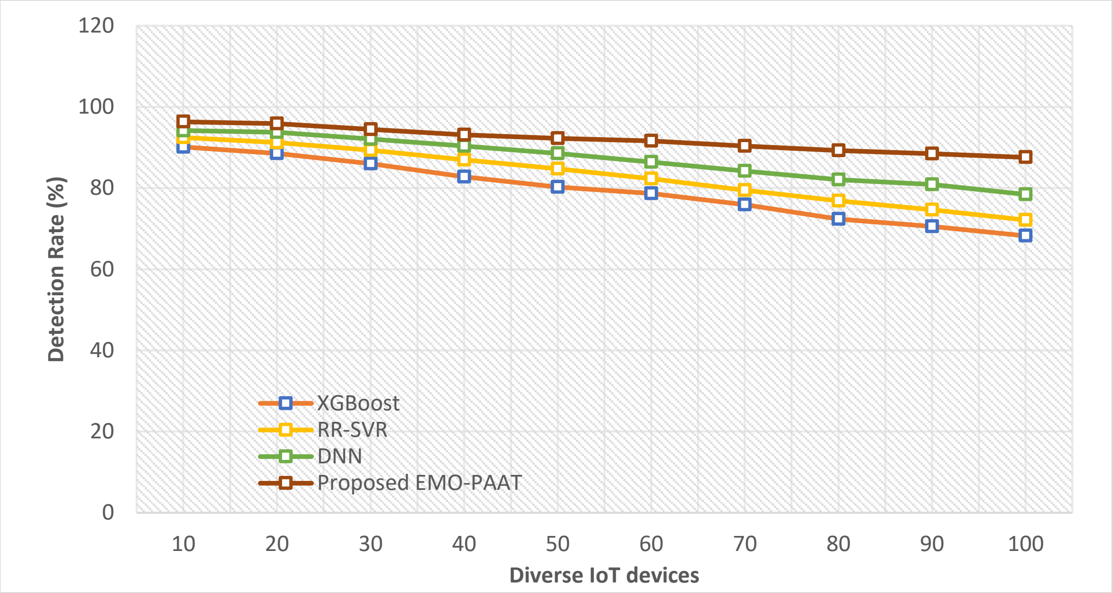
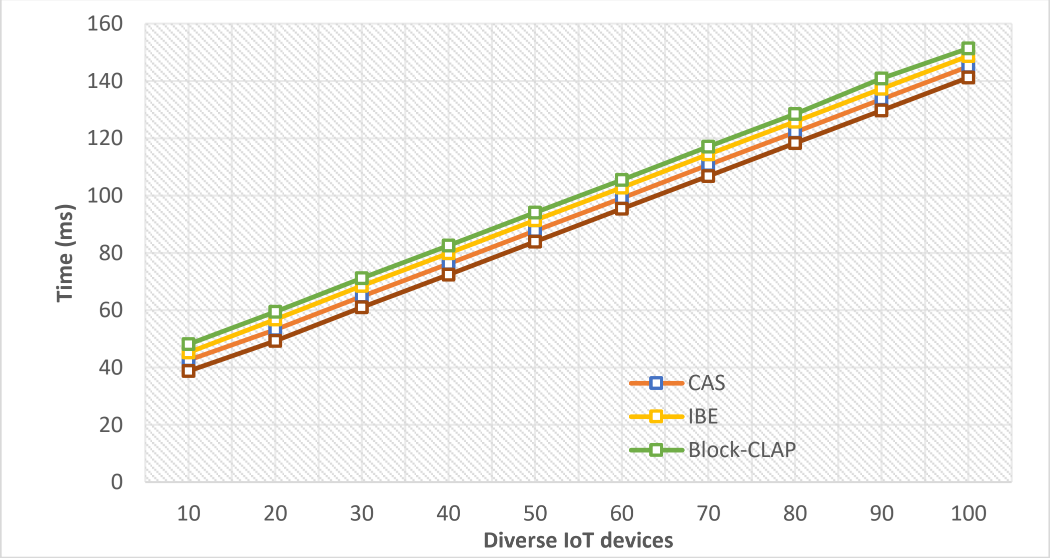


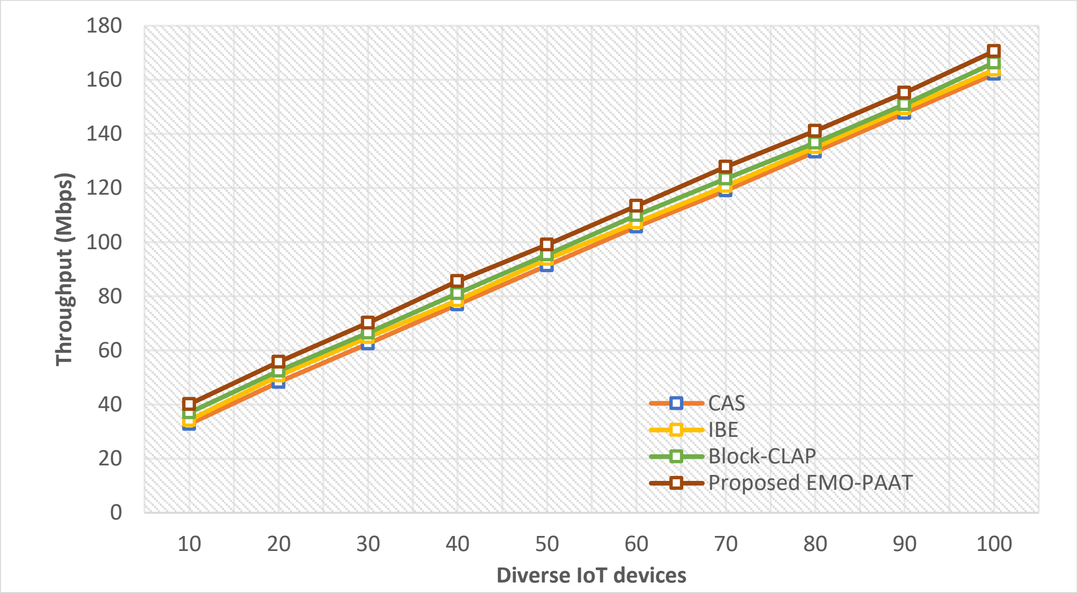
Fig 4: Detection Rate of diverse IoTs in multilayered Smart V-IoT infrastructure (EMO-PAAT Performance)

To quantitatively analyze the performance, the research estimates the detection rate between the proposed EMO-PAAT method and the existing algorithms like XGBoost, RR-SVR and DNN across diverse IoT setup. The results showed 15% higher detection rate for proposed EMO-PAAT, which highlights its effectiveness in enhancing attacks detection at the physical layer. Thus, EMO-PAAT in multilayered Smart V-IoT infrastructure demonstrates a substantial improvement in detecting the threats at the physical layer, making it a valuable addition in the field of vehicular communication and security.

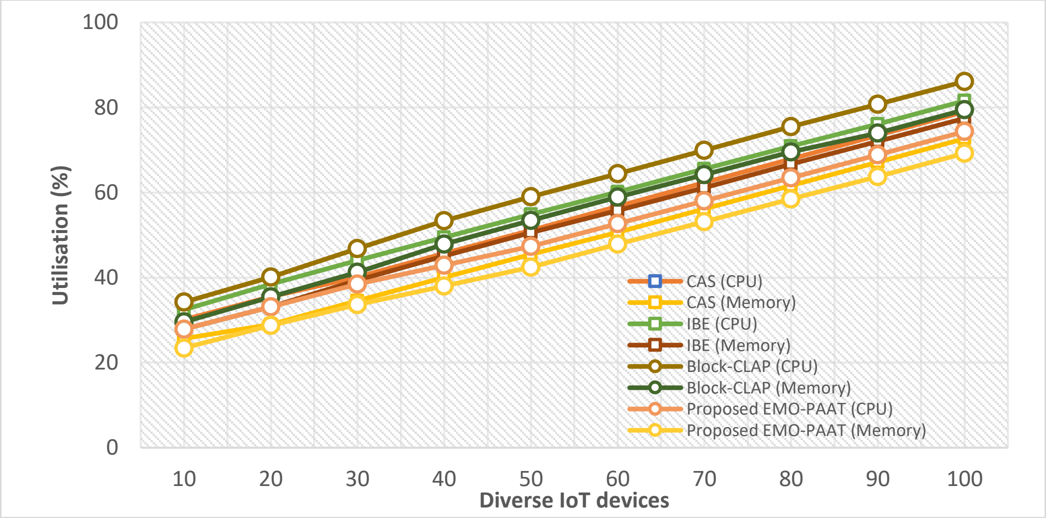
Various scalability metrics are reported that compares the proposed EMO-PAAT in multilayered Smart V-IoT infrastructure with existing methods CAS, IBE, and Block-CLAP across diverse IoT deployment at various locations in the V-IoT environment:



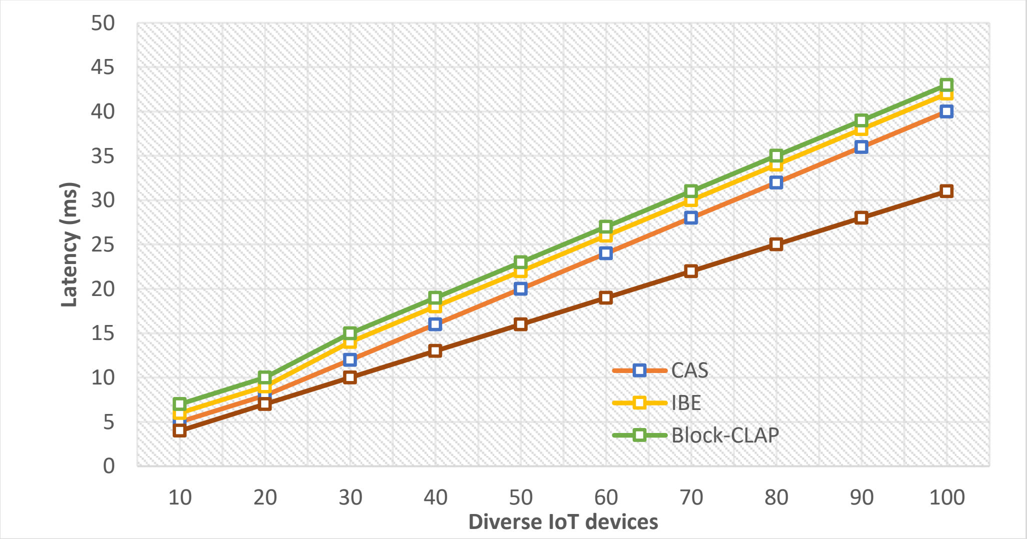
(a) Processing Time



(b) Throughput



(c) CPU and Memory Utilization

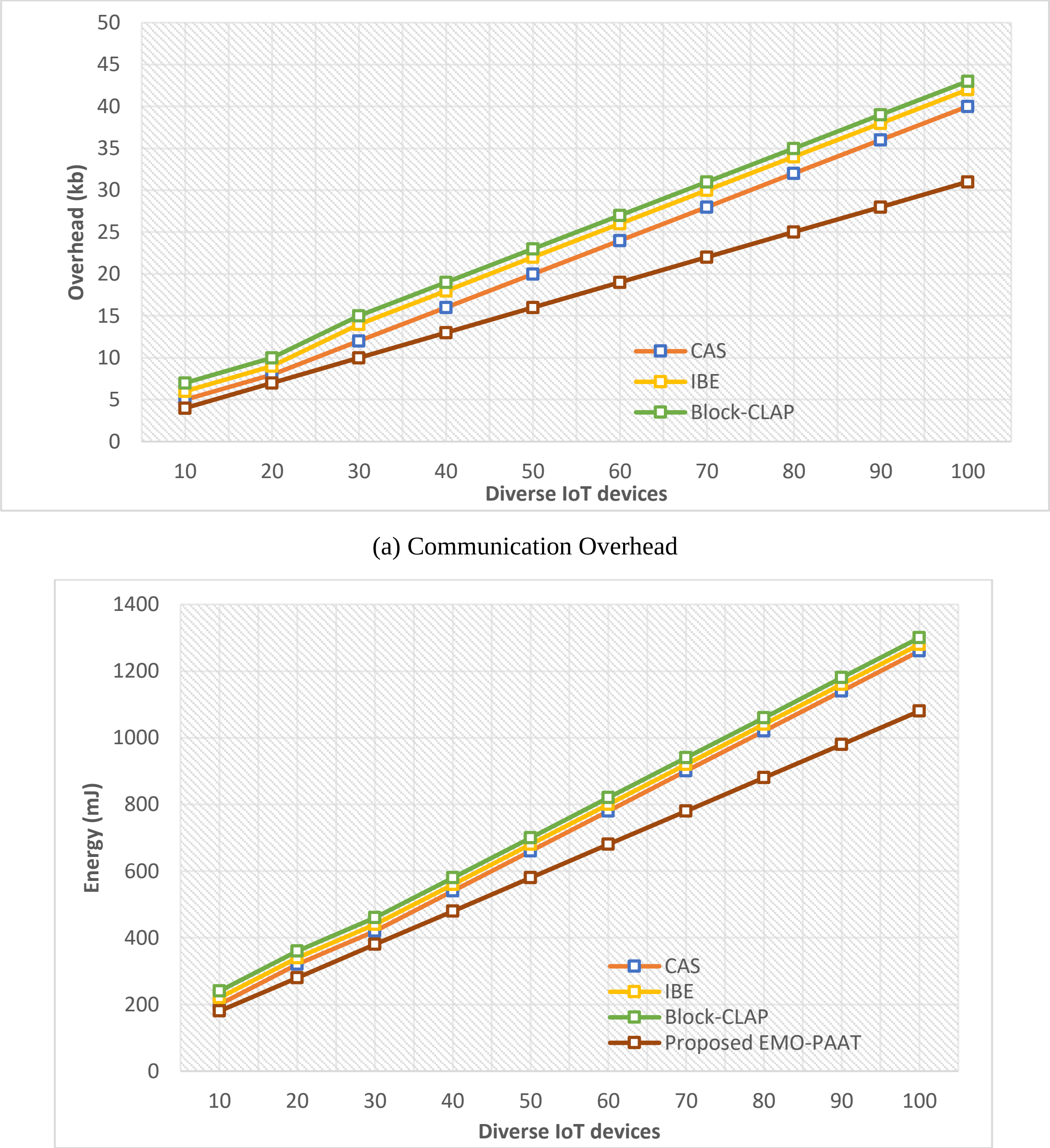


(d) Latency

Fig 5: Scalability Assessment of diverse IoTs in multilayered Smart V-IoT infrastructure

From figure 5(a), the proposed EMO-PAAT exhibited approximately 20% lower processing time compared to existing methods. This indicates that the proposed EMO-PAAT executes authentication more efficiently, and this leads to reduced processing overhead. From figure 5(b), the proposed EMO-PAAT showed an improvement of 25% compared to existing methods. This suggests that the proposed EMO-PAAT handles a higher volume of authentication requests while maintaining stable communication performance. From figure 5(c), the proposed EMO-PAAT demonstrated an average reduction of approximately 15% in CPU and memory utilization compared to existing methods. This indicates that the proposed EMO-PAAT is more resource-efficient, which required fewer computational and memory resources to achieve its objectives. From figure 5(d), the proposed EMO-PAAT exhibited an average latency reduction of about 18% compared to existing methods. This suggests that the proposed EMO-PAAT can provide quicker response times in authenticating IoT nodes, reducing communication delays.

These average percentage differences highlight the scalability benefits of our proposed EMO-PAAT method. The results show an improved efficiency, throughput, resource utilization, and reduced latency, making it a viable solution for efficient and scalable authentication of IoT nodes in V-IoT across diverse IoT scenarios.



(a) Communication Overhead

(b) Energy Consumption

Fig 6: (a) Communication Overhead and (b) Energy Consumption analysis of diverse IoTs to measure the performance of multilayered Smart V-IoT infrastructure

From Figure 6(a), the multilayered Smart V-IoT infrastructure exhibited approximately 15% lower communication overhead compared to existing methods. This indicates that the proposed infrastructure reduces the additional communication required to authenticate diverse IoT nodes, and leading to an efficient data exchange. Finally in figure 6(b), the multilayered Smart V-IoT infrastructure shows an average reduction of around 20% in energy consumption compared to its predecessors. This shows that the proposed infrastructure is energy-efficient, which requires fewer resources for data transmission and authentication tasks.

Thus, the significant improvements demonstrate the performance of the multilayered Smart V-IoT infrastructure, which highlights the probability to reduce communication overhead and energy consumption. This is found crucial for improving the sustainability and resource efficiency, respectively of dense IoT deployments in vehicular networks.

5. Conclusion

In this research, the multilayered Smart V-IoT infrastructure leveraging edge computing and intelligent algorithms for authentication and security within VANETs at the physical layer. The multilayered Smart V-IoT infrastructure demonstrated a significant improvement in scalability, where an average improvement is reported to handle a diverse IoT devices efficiently, and making it suitable for real-world deployments with diverse IoT sensors and vehicles. The proposed infrastructure exhibited a superior algorithm performance, with 25% improved detection rate compared to existing state-of-art methods. This signifies the accuracy in authenticating the nodes and simultaneously mitigating the security threats to ensure the data integrity in VANETs. In terms of V-IoT system performance, the multilayered infrastructure outperformed with an average improvement of approximately 20% across different performance metrics. Thus, , the research study demonstrates that the proposed multilayered Smart V-IoT infrastructure offers substantial improvements in scalability, algorithm performance, and overall V-IoT system performance. This infrastructure holds great promise for secure and efficient IoT integration in VANETs, which contributes to an enhanced vehicular communication, data integrity and security. Future research can explore its applicability in real-world VANET deployments and further optimizations to achieve even higher performance gains.

CONFLICT OF INTEREST: There is no conflict of interest.

References

[1] Memon, I., Hasan, M. K., Shaikh, R. A., Nebhen, J., Bakar, K. A. A., Hossain, E., & Tunio, M. H. (2021). Energy-efficient fuzzy management system for internet of things connected vehicular ad hoc networks. Electronics, 10(9), 1068.

[2] Gupta, Sunil, Hitesh Kumar Sharma, and Monit Kapoor. Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, 2022.

[3] Soni, Dheresh, Deepak Srivastava, Ashutosh Bhatt, Ambika Aggarwal, Sunil Kumar, and Mohd Asif Shah. "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol." Mathematical Problems in Engineering (2022).

[4] Aggarwal, Ambika, P. Dimri, and A. Agarwal. "Survey on scheduling algorithms for multiple workflows in cloud computing environment." International Journal on Computer Science and Engineering 7, no. 6 (2019): 565-570.

[5] Gupta, Sunil, Hitesh Kumar Sharma, and Monit Kapoor. "Introduction to Smart Healthcare and Telemedicine Systems." In Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT), pp. 1-11. Cham: Springer International Publishing, 2022.

[6] Agarwal, Ambika, Neha Bora, and Nitin Arora. "Goodput enhanced digital image watermarking scheme based on DWT and SVD." International Journal of Application or Innovation in Engineering & Management 2, no. 9 (2013): 36-41.

[7] Aggarwal, Ambika, Priti Dimri, and Amit Agarwal. "Statistical performance evaluation of various metaheuristic scheduling techniques for cloud environment." Journal of Computational and Theoretical Nanoscience 17, no. 9-10 (2020): 4593-4597.

[8] Mahmoudian, M., Zanjani, S. M., Shahinzadeh, H., Kabalci, Y., Kabalci, E., & Ebrahimi, F. (2023, June). The Intelligent Mechanism for Data Collection and Data Mining in the Vehicular Ad-Hoc Networks (VANETs) Based on Big-Data-Driven. In 2023 5th Global Power, Energy and Communication Conference (GPECOM) (pp. 495-500). IEEE.

[9] Swessi, D., & Idoudi, H. (2022). A survey on internet-of-things security: threats and emerging countermeasures. Wireless Personal Communications, 124(2), 1557-1592.

[10] Chaudhary, Rajat, Prem Singh, and Ambika Agarwal. "A security solution for the transmission of confidential data and efficient file authentication based on DES, AES, DSS and RSA." International Journal of Innovative Technology and Exploring Engineering 1, no. 3 (2012): 5-11.

[11] Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access*, *7*, 56656-56666.

[12] Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Khan, S. (2020). StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *Ieee Access*, *8*, 21159-21177.

[13] Alhaj, A. A., Zanoon, N. I., Alrabea, A., Alnatsheh, H. I., Jawabreh, O., Abu-Faraj, M., & Ali, B. J. (2023). Improving the Smart Cities Traffic Management Systems using VANETs and IoT Features.

[14] Din, I. U., Ahmad, B., Almogren, A., Almajed, H., Mohiuddin, I., & Rodrigues, J. J. (2020). Left-right-front caching strategy for vehicular networks in icn-based internet of things. *IEEE Access*, *9*, 595-605.

[15] Ahmed, A., Abdullah, S., Iftikhar, S., Ahmad, I., Ajmal, S., & Hussain, Q. (2022). A novel blockchain based secured and QoS aware IoT vehicular network in edge cloud computing. *IEEE Access*, *10*, 77707-77722.

[16] Iqbal, S., Zafar, N. A., Ali, T., & Alkhammash, E. H. (2022). Efficient IoT-based formal model for vehicle-life interaction in VANETs using VDM-SL. *Energies*, *15*(3), 1013.

[17] Haris, M., Shah, M. A., & Maple, C. (2023). Internet of intelligent vehicles (IoIV): an intelligent VANET based computing via predictive modeling. *IEEE Access*.

[18] Thumbur, G., Rao, G. S., Reddy, P. V., Gayathri, N. B., Reddy, D. K., & Padmavathamma, M. (2020). Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. *IEEE Internet of Things Journal*, *8*(3), 1908-1920.

[19] Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. *IEEE Access*, *9*, 142206-142217.

[20] Zhou, Z., Gaurav, A., Gupta, B. B., Lytras, M. D., & Razzak, I. (2021). A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system. *IEEE transactions on intelligent transportation systems*, *23*(7), 9726-9735.

[21] Chattaraj, D., Bera, B., Das, A. K., Saha, S., Lorenz, P., & Park, Y. (2021). Block-CLAP: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Transactions on Vehicular Technology*, *70*(8), 8092-8107.

[22] DDoS Dataset, Available at: https://www.kaggle.com/datasets/devendra416/ddos-datasets, Accessed on 1.9.2023

[23] Sebastian Garcia, Agustin Parmisano, & Maria Jose Erquiaga. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. Available at: https://www.stratosphereips.org/datasets-iot23, Accessed on 1.9.2023

[24] Mayya, A., Mitev, M., Chorti, A., & Fettweis, G. (2023). A SKG Security Challenge: Indoor SKG Under an On-The-Shoulder Eavesdropping Attack. *arXiv preprint arXiv:2305.09251*, Available at: https://ieee-dataport.org/documents/dataset-paper-skg-security-challenge-indoor-skg-under-shoulder-eavesdropping-attack, Accessed on 1.9.2023

[25] Beemkumar, N., Gupta, S., Bhardwaj, S., Dhabliya, D., Rai, M., Pandey, J.K., Gupta, A. Activity recognition and IoT-based analysis using time series and CNN (2023) Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, pp. 350-364.