Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing Multi-Layered Vehicular Internet of Things (V-IoT) Communication using Enhanced Authentication and Threat Detection with Conditional Decision Trees and Hunting Search

Pratima Upadhyay [1], Dr. Samta Jain Goyal [2], Dr. Venkatadri Marriboyina [3]

[1]Research Scholar, Department of Computer Science & Engineering, Amity School of Engineering and Technology, Amity University, Gwalior. Madhya-Pradesh, India.
Email Id: pratimaupadhyay784@gmail.com
[2]Associate Professor, Dept. of CSE, Amity University, Gwalior (M.P.) India.
Email Id: sjgoyal@gwa.amity.edu
[3]Associate Dean and Professor, Dept. of CSE, NMIMS, Shirpur, Maharashtra, India.
Email Id: Venkatadri.mr@gmail.com

In evolving technology, the combination of vehicular ad-hoc networks (VANETs) architecture with Internet of Things (IoT) devices in intelligent transportation systems (ITSs) added a new dimension for reliable data communication. The challenge of secured IoT node addition while mitigating eavesdropping, denial of service (DoS), and malware attacks remains a concern in establishing reliable communication links. The VANET-IoT (V-IoT) system is developed in this research to support scalable communication with increasing IoT devices and to evade further risks to device usage without compromising security.

Ensuring secured node authentication in V-IoT facilitates the admittance of newer IoT devices to the VANET infrastructure is the main objective of the research. Conventional methods fail to maintain a trade-off between threat detection and authentication via edge networks to ensure secure and reliable communication. To mitigate such challenges, the present research develops a multi-layered V-IoT infrastructure to incorporate crucial components of reliability and security like authentication, IoT devices, edge computing, and threat classification using the combination of conditional decision trees (CDT) and hunting search (HS). The former acts as an authenticator, and the latter acts as a threat classifier, which identifies eavesdropping, denial of service (DoS), and malware attempts in V-IoT systems. Further, edge computing is leveraged to integrate the CDT-HS into the V-IoT system for authentication of IoT devices and threat detection. The proposed method is evaluated in terms of various parameters like edge and V-IoT processing and scalability using different metrics like throughput, processing time, CPU and memory utilization, detection rate, latency, energy consumption, and communication overhead. The results show a significant improvement in ensuring reliable and secured communication in V-IoT systems.

Keywords: Security, V-IoT, VANETs, Authentication, Conditional Decision Trees, Hunting Trees

1. Introduction

In the current era, the advancement in integrating Internet of Things (IoT) devices into Vehicular Ad-Hoc Networks (VANETs) infrastructure has transformed the process of data communication reliably and securely [1]. Such integration develops a new infrastructure called the Vehicular Internet of Things (V-IoT), providing enhanced intelligence and connectivity across Intelligent Transportation Networks [2]. However, it undergoes a series of challenges, which are primarily focused on securing the network while newer IoT nodes are added inside the network and evading against the potential threats within the V-IoT infrastructure [3].

VANETs can maintain communication networks intelligently among vehicles in a dynamic and complex way during the IoT device integration in VANET [4]. The incorporation of IoTs in VANETs improves the functionalities of the transportation system, but it suffers from vulnerabilities that are manipulated by malicious entities [5,6]. The conventional V-IoT architecture is designed to enhance IoT integration and scalability, however, it suffers from security issues associated with the increasing use of devices [7]. This vulnerability exposes the network to be susceptible to various forms of threats [8].

The complexities associated with maintaining communication security increase with increasing number of communications associated with increasing IoT devices [9]. Initially, the V-IoT architecture must be suitable for the seamless addition of IoT devices and then it should support high-level security without compromising the network security [10]. This objective demands a trade-off between the authentication and scalability of the network [11]. Finally, the V-IoT architecture exhibits resilience against potential vulnerabilities against eavesdropping, DoS attacks, and malware [12]. These threats have the ability to compromise the availability and integrity of critical data in V-IoT infrastructure [13].

The research aims to design a novel multi-layered V-IoT framework that facilitates dynamic IoT node addition and proactively mitigates the threats. It enables a seamless authentication and secured addition that verifies the IoT device identification. Further, the threat detection mechanism identifies and mitigates the eavesdropping, DoS attacks, and malware. The entire computations are carried out in edge controller that enables a real-time authentication and threat detection.

A novel approach is designed to secure the communication in multi-layered V-IoT framework (Figure 1) that combines Conditional Decision Trees (CDT) and Hunting Search (HS). The former enables authentication and provides robust verification of IoT node addition. The latter acts as a threat classifier, where the entire functionality of V-IoT is conducted via edge computing.

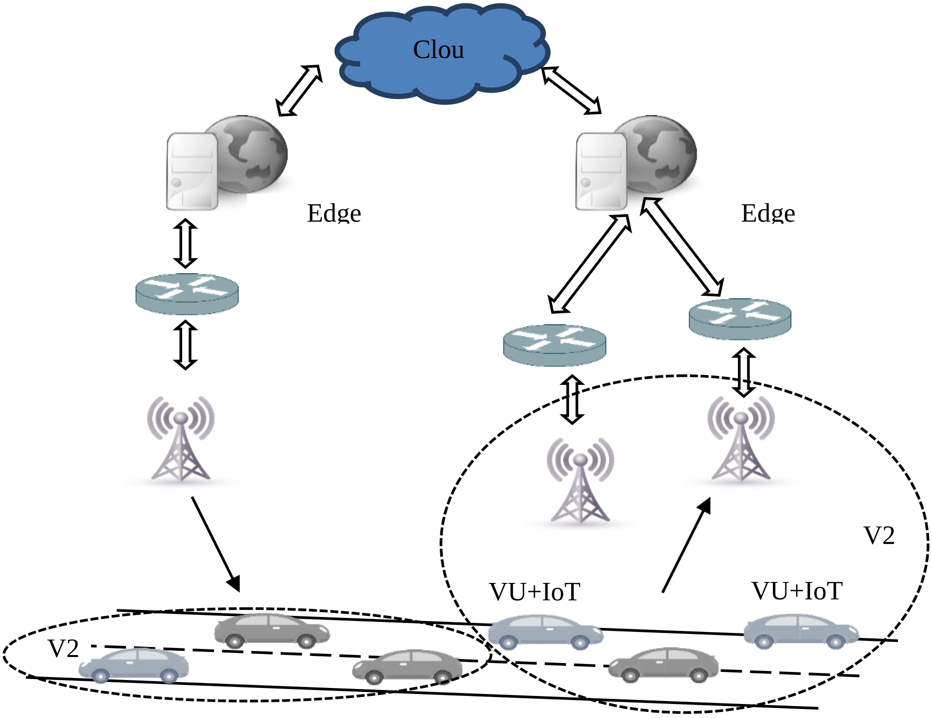

Figure 1: V-IoT Architecture

The main contribution of the research involves the following:

- The authors develop a Multi-Layered V-IoT Infrastructure with Edge Computing Technology to establish seamless and secured communication in VANETS via IoT devices.
- The research uses a novel Vehicular Message Queue Telemetry Transport (V-MQTT) protocol to enable auto-configuration for secured and seamless device connectivity.
- The edge computing acts as a main controller that authenticates the IoT node's addition in V-IoT Infrastructure. The V-IoT ensures low-latent and high-bandwidth communication, which is considered crucial for high-speed data transmission from IoT devices to Centralized Server (CS) or Software-Defined Networking (SDN)/Storage Controllers (SC).

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

Related Works

In this section, various methods of integrating IoT/edge across VANETs are discussed while maintaining the security of the network in a robust manner. The summary of which are given below and a short summary is presented in Table 1.

The need for higher efficiency and productivity is considered critical in heterogeneous IoT networks since it lack a reliable authentication protocol in VANETS. This is found essential for secured communication of data between IoT nodes. In order to secure the network against various threats like replay/man-in-the-middle attacks, an online/offline lightweight authentication technique is proposed in [14] using the AES-RSA algorithm. By including offline joining, you can protect your network from outside attacks and lessen the likelihood of service disruptions as you move between countries. The combination of offline combination enables the network to prevent various remote intrusions and risks associated with secured connectivity during transitions between the secured network boundaries. In [15], the authors study an emergency reporting system in VANET with IoT as its integral component. A Mult signature-architecture is developed to increase the security and traffic management with proper recognition on authentic emergency messages. The research develops a onboard unit (OBU) in a secured manner that utilizes an emergency reporting scheme and it is named as SOERS. This scheme is beneficial in reducing the computation and transmission overhead via aggregation of signatures. It further overcome the limitations presented of existing reporting methods in mitigating the malicious entities that spread hoaxes during genuine emergencies for financial benefit. The need of security and privacy is studied in [16] for VANETs that has prompted an authentication mechanism. Quotient Filter (QF) is utilized for the authentication of nodes and Elliptic Curve Cryptography (ECC) is used for the authentication of message, where these two methods increase the VANET security. This assigns a unique pseudo identity to vehicles and this helps to protect the users. The Fog Nodes (FN) deployment in associated with RSUs, where it reduces the latency and increases the system throughput to offer a protective environment against unauthorized vehicle nodes and incorrect communications. In [17], a connection is established between IoT and VANETs that focus on reducing the load in Software Defined Network (SDNs) architecture. A private collaborative intrusion detection system (p-CIDS) is developed with group authentication scheme to form an energy-efficient security for SDVNs. The combination of group ID-key pairs and collaborative learning enables private communication for intrusion detection while homomorphic encryption and differential privacy maintains the security of the data.

In [18], the incorporation of cloud computing with VANETs allows the vehicle to pool the network resources. It offers data access for intelligent decision making and this architecture uses VANET in the cloud for available resource identification and to utilize the Internet of Vehicles (IoV) software. Additionally, the research provides real-time access to a cloud-based VANET to employ a distributed method for improved communication security. In [19], the authors emphasize continuous sensor data-based vehicle-to-vehicle communication in VANETs. It improves the security using deep learning and then a trust model is developed to migrate the data to the vehicular cloud. Further, trust-based federated transfer quadratic authentication is appended to the IoT-based VANETs to increase the piloted vehicle security.

The results show an improved throughput, reduced latency, data transfer rate, and scalability. Finally, the combination of VANETs, cloud computing, and the IoT creates a next-generation smart city [20]. The VCoT framework integrates IoT with vehicular networking clouds to develop a communication design that focus on LoRaWAN communication protocol to addresses the issues such security, data aggregation, data quality, privacy and network coverage.

The problems discussed above is examined in this research that pertains in the lack of an architecture to secure the communications and authentication in smart V-IoT infrastructure. The Conventional approaches do not provide a comprehensive solution that effectively combines IoT node authentication and detection of various threat via an edge controller.

Table 1: Summary of Existing VANET Integration other Disruptive Technologies and its related Performance

Ref.	VANET Architecture	Method	Performance Metrics	Outcomes
[14]	Cross-domain VANET in IIoT	AES-RSA	Computation and communication cost	Outperforms ID-CPPA, AAAS, and HCDA
[15]	Emergency Reporting System	Multi-signature	Computation and communication overhead	Efficient solution for secure emergency reporting
[16]	Secure and Privacy-Preserving Authentication	Quotient Filter (QF), ECC	Node and message authentication	Identifies illegitimate vehicle nodes
[17]	SDVN for IIoT in VANETs	Group authentication, private intrusion detection (GAPID) system	Energy efficiency, communication overhead	Increased energy efficiency, accurate intrusion detection
[18]	Cloud-based VANET (CVANET)	Cloud computing, IoV application management	Security algorithm	Real-time access to IoV
[19]	Security in VANET with Cloud-based Navigation	Deep learning, trust model	Throughput, data transmission rate, latency	Improved security
[20]	Vehicular Clouds with IoT (VCoT)	LoRaWAN-based vehicular networks	Network traffic analysis, scalability	Enriched services for smart city applications

Proposed Multi-Layered Smart V-IoT Infrastructure

In this section, the proposed V-IoT communication infrastructure combines IoT architecture for data collection, edge computing with CDT for device authentication, and HS for threat detection, where it offers a solution for dynamic node addition and mitigation of cyber threats. The architecture of the proposed Multi-Layered Smart V-IoT Infrastructure is illustrated in Figure 2.

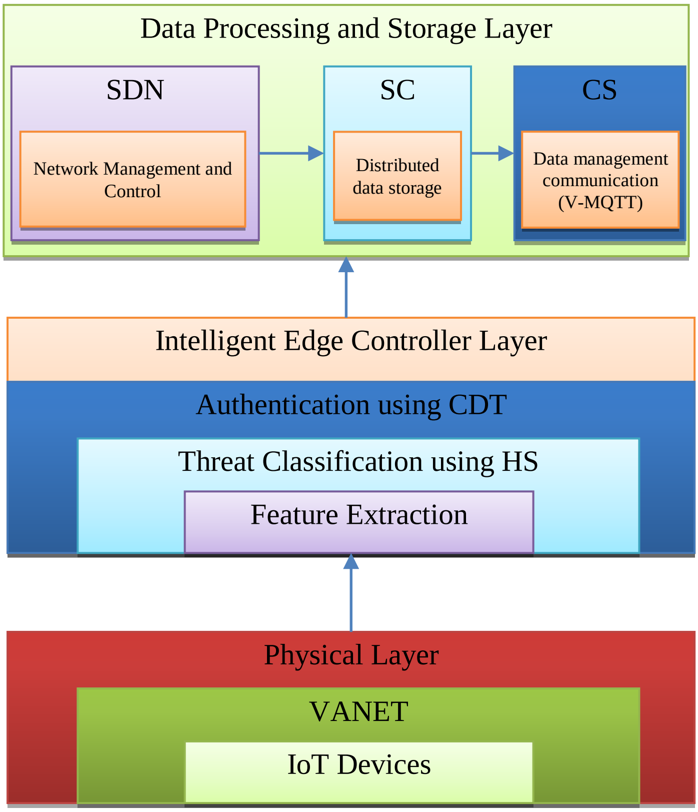
Data Processing and Storage Layer
SDN
Network Management and Control
SC
Distributed data storage
CS
Data management communication (V-MQTT)
Intelligent Edge Controller Layer
Authentication using CDT
Threat Classification using HS
Feature Extraction
Physical Layer
VANET
IoT Devices

Figure 2: Multi-Layered Smart V-IoT Infrastructure

1.1. System Model

The proposed method combines diverse IoT devices of different configurations in the VANET infrastructure. These devices communicate via the V-MQTT protocol, which is designed specifically to fit the communication within the VANET environment. The V-MQTT enables auto-configuration that offers the ability to connect and communicate in a seamless manner. To achieve this, the research studies the diversity of IoT devices and their adoption with VANETs via V-MQTT protocol for seamless and secured connectivity.

Diversity (D) of IoT Devices: Various IoT devices are embedded with Vehicles Units (VUs) or RSUs, hence the diversity (*D*) pattern is studied while the devices communicate with the proposed V-MQTT protocol. It further studies the allowable IoT sensor device types, and its required communication capabilities using Eq.(1)

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

where, N_t - number of IoT sensor types, N_i - number of instances captured by each IoT sensor type, C_{ij} - communication capability of type *i* on an index *j*, and $j \in [1\text{-}3]$ - index of *i* or the range of IoT devices with various capabilities like low, medium and high.

VANET Configuration (VC): The VC (Eq.(2)) involves the parameters of VU/RSU to establish seamless connectivity with the IoT devices using different factors like transmission power, communication range and network topology.

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

where, N - parameters of VANET configuration, P_i - i^{th} parameter (i.e. communication range, transmission power), R_i - range associated with i^{th} parameter.

Table 2: VANET Configuration Parameters with V-MQTT protocol

IoT Device	**Transmission Power (P_i) dBm**	**Communication Range (R_i) in meters**	**Network Topology**
GPS Tracker	20	150	Mesh
OBD-II Dongle	15	100	Star
Camera Module	25	200	Clustered
Temperature Sensor	10	50	Ad Hoc
Lidar Sensor	30	250	Mesh
Tyre Pressure Sensor	12	80	Mesh
Speed Sensor	18	120	Ad Hoc

1.1.1. V-MQTT Modelling:

V-MQTT is developed as a lightweight communication protocol to support seamless communication for the IoT devices in V-IoT environment. It uses unique features or factors of VANETS including its varying signal strengths, high mobility, location-based information, real-time communication, and intermittent connectivity. The IoT device within the VU communicates using this protocol to the V-MQTT client for publishing/subscribing to a topic. The entire communication protocol operates based on the transmit power and strength of a IoT device that considers signal attenuation factor for high-speed communication. The V-MQTT uses a publish-subscribe model, where the IoT devices aim to publish/subscribe messages to transmit/receive messages between VU/RSU. V-MQTT model is highly suited for communication among multiple IoT devices, where it receives continued updates/events from an RSU/VU/other IoT source. V-MQTT further integrates authentication and security features to exchange messages between the devices, which is considered crucial while connecting vehicles with IoT devices to transmit sensitive information.

The transmission power or range of an IoT device in a VU is represented as a parameter P_t, which is expressed in Eq. (3):

$$P_t = \min(P_t) + \alpha\times(\max(P_t) - \min(P_t)) \qquad (3)$$

where $\min(P_t)$ - minimum transmission power; $\max(P_t)$ - maximum transmission power; α = [0, 1] - factor representing the transmission power modulation.

The communication range is estimated using the transmission power along the free-space path loss model, which is expressed in Eq.(4):

$$R = \sqrt{\frac{P_t}{PL}} \qquad (4)$$

Where P_L - path loss factor.

The IoT device behavior in V-MQTT protocol is modeled using MQTT principles including publishing and subscribing to topics. For instance, each IoT device is intended to publish the data it collects or to subscribe the data from RSU to control the VU based on the following expression in Eq.(5) and Eq.(6), respectively.

$$P_{pub} = \sum_{x,VU} \frac{N_{x_{VU},pub}}{T_{x_{VU},pub}} \quad (5)$$

$$P_{sub} = \sum_{x,VU} \frac{N_{x_{VU},sub}}{T_{x_{VU},sub}} \quad (6)$$

Where P_{pub} - publishing rate of an IoT device x, P_{sub} - subscribing rate of an IoT device x, N_{pub} - number of published messages of an IoT device x, N_{sub} - number of subscribed messages of an IoT device x, T_{pub} - time taken for publishing a message by an IoT device x, and T_{sub} - time taken for subscribing to a message by an IoT device x.

The messages are normally encrypted using cryptographic encryption while getting transmitted and it is then decrypted using the following expression as in Eq.(7) and Eq.(8):

$$C=E(K,P) \quad (7)$$

$$P=D(K,C) \quad (8)$$

Where C - ciphertext, P - plaintext, K - encryption key, E - encryption function, and D - decryption function.

Further, to include the location of the VU in V-MQTT model, GPS coordinates are utilized and the distance is estimated using Eq.(9):

$$D = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2} \quad (9)$$

Where (x_1,y_1) and (x_2,y_2) are the coordinates of two locations.

1.2. Edge Computing (Controller)

Edge computing involves feature extraction-based authentication and threat detection in edge servers using CDT and HS, respectively.

1.2.1. CDT Authentication

The CDT authentication (ref. Figure 3) ensures the dynamic and secured addition of IoT nodes into V-IoT. CDT is used as an authenticator to verify the authenticity of IoTs inside VU when entering the network. The ability of CDT decision making ability evaluates different conditions of IoT devices in the network prior granting authentication, where it enhances the reliability of the devices getting authenticated. Such efficient onboarding of devices ensures a trade-off between the security and flexibility.

Each decision tree node signifies the decision made using specific attribute of IoT device, where the conditions are modelled using if-then rule, where conditions are evaluated in the tree branches of varying paths. While making decisions, the CDT splits the data into decision nodes and creates a data subset, which are homogenous w.r.t target variable. The CDT has the ability to handle different conditions/features of a IoT device during its authentication phase, and this includes numerical values, categorical variables, or combinations of both. This is highly suitable for decision making and can adapt with diverse data. The tree grows when the data is recursively split into subsets based on the condition and this process continues until the minimum data points are reached.

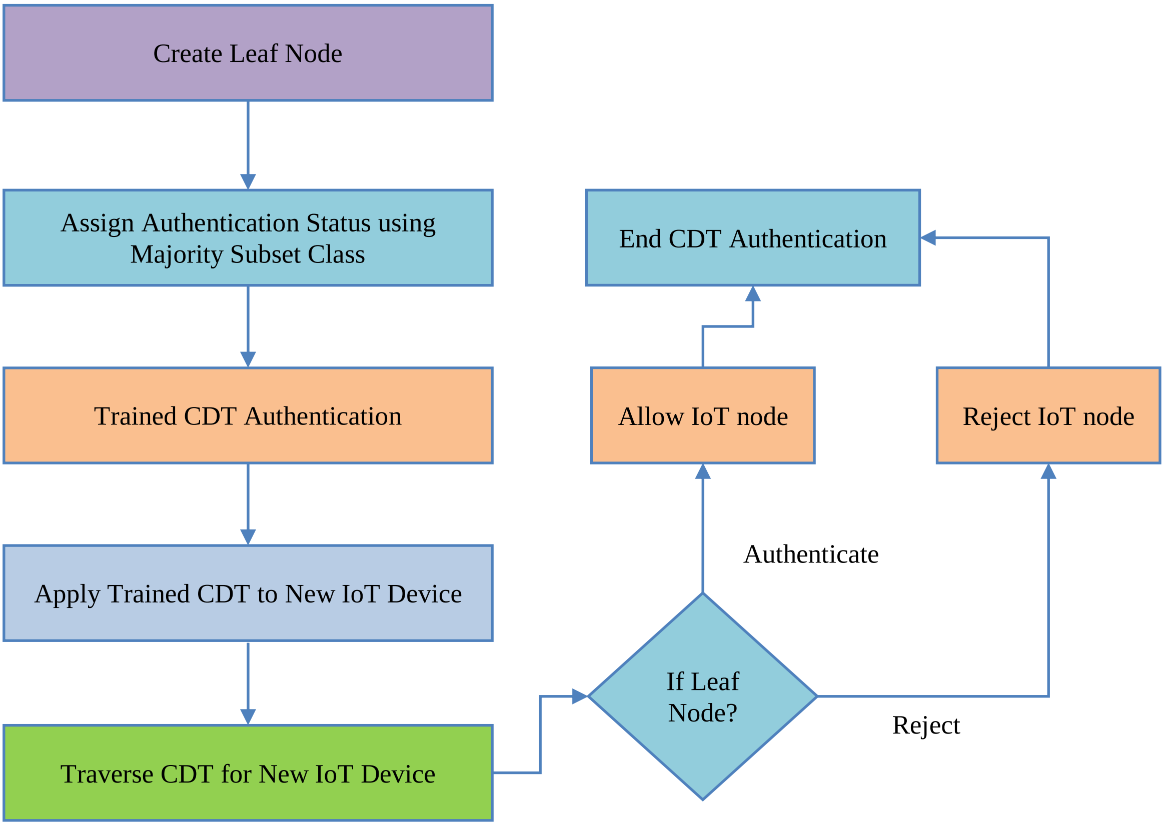
Create Leaf Node
Assign Authentication Status using Majority Subset Class
Trained CDT Authentication
Apply Trained CDT to New IoT Device
Traverse CDT for New IoT Device
If Leaf Node?
Authenticate
Reject
Allow IoT node
Reject IoT node
End CDT Authentication

Figure 3: CDT Authentication Process Flow

CDT Authentication uses CDT for authenticating IoT entities within V-IoT, where it amends the conditional decision tree to verify the IoT device identity that seeks to join the network. The features used for authentication are closely related to the IoT device identity. It includes device IDs, cryptographic credentials, authentication keys, or other relevant information. Depending on these features, the decision nodes are conditioned. For instance, a decision node evaluates whether the cryptographic credentials of an IoT device match the predefined values. The splitting criteria get evaluated to find if the splitting is required to authenticate or categorize the IoT devices using features threshold to create device subsets. This facilitates secured IoT node addition.

CDT Authentication Process

Input: Training dataset *D* with *X* features from a IoT device *x* identity and labels *y* indicating the status of authentication; Stopping criteria: minimum samples per leaf.

Output: Trained CDT for authentication.

```
a)  If stopping criteria is met:
    i)   Create a leaf node
    ii)  Assign the authentication status using majority subset class.
b)  Else
    i)   Select Best Splitting Criterion
         (1)  For feature $X_i$,
              (a)  calculate impurity measure for each threshold ($T$).
         (2)  Select feature $X_i$ and $T$ to reduce impurity.
    ii)  Split the Dataset $D$ into two subsets $D_{left}$ and $D_{right}$ using $X_i$ and $T$.
         (1)  Formulate the node condition as $X_i \leq T$
    iii) Recursive Call - Left Branch
```

```
            (1)  Apply the CDT Authentication recursively to the subset $D_{left}$.
            (2)  Create a node condition as $X_i \leq T$
                 (a)  Connect with left branch.
        iv)  Recursive Call - Right Branch:
            (1)  Apply the CDT Authentication algorithm recursively to the subset $D_{right}$
            (2)  Create a node condition as $X_i > T$
                 (a)  Connect with right branch.
2)  Return the trained CDT for authentication.
3)  Apply Trained CDT to New IoT Device with feature $X$ (device ID, cryptographic credentials)
4)  Traverse CDT using each node conditions for $X$ of a new IoT in VU
    a)  Continue traversing until it reaches the leaf node
5)  If Leaf Node:
    a)  Authenticate, grant access.
6)  If Leaf Node:
    a)  Reject, deny access.
```

1.3. HS Threat Classification

The algorithm initiates with the initial population, which represents possible solutions in the V-IoT environment. Consider P as the population of possible configuration in V-IoT: $P=\{p_1, p_2, \ldots, p_n\}$ with n being the population size. The research defines an objective function $f(p)$ (Eq.(10)) to classify the attack in the V-IoT system for each population $p \in P$, where p represents the possible solution. $f(p)$ evaluates the fitness of the population based on unexpected network traffic, abnormal behavior patterns, and known signatures of threats.

HS imitates the hunting behavior, wherein the prey represents threats during the threat detection process in the V-IoT system. The HS uses a search strategy, which is inspired from the behavior of predators to adapt its hunting ability w.r.t change in environment and their prey behavior. depending on the previous behavior of predators and its respective environmental changes, the algorithm dynamically adjusts the solution. The search space is hence represented as Sp for each solution p, where HS adapts dynamically the Sp during its search process.

To adapt dynamic behavior, the exploration and exploitation are balanced to navigate Sp. The HS then adapts with these changes in the threat V-IoT environment and allows it to find the known and novel threats. It then classifies the solution p using the objective function evaluation, where if $f(p) > T$, the solution p is classified as the potential threat.

$$f(p) = \sum_{i=1}^{k} w_i \cdot g_i\left(p\right) \qquad (10)$$

where, k - total of features used in the threat detection; w_i- weight assigned to the i^{th} feature; $g_i(p)$ - function that quantifies the threat level using i^{th} feature for solution p.

The HS classifies the normal and anomalous behavior, where it identifies the DoS attack instances, the presence of malware or eavesdropping attempts. The efficacy of the previous solution is modified based on dynamic adjustment over parameters and strategies, which allows HS to improve its threat detection capabilities.

```
HS Threat Classification
Input: $P$ , $f(p)$ and Stopping criteria
Output: Identified threats
    1.  Initialize a population $P$, exploration rate, adaptation factors, and search space.
    2.  Evaluate threat level for $p \in P$ using $f(p)$.
    3.  Mimic hunting behavior with dynamic adjustment of search space.
            •  Update the exploration rate
            •  Update adaptation factors using previous solutions and environmental changes.
    4.  Adapt search parameters, exploration, and exploitation strategies dynamically.
            •  Balance exploration/exploitation using changing threat space.
    5.  Classify solution using objective function.
            •  Identify solutions that surpass a threat threshold as potential threats.
    6.  Dynamic Adjustment: Dynamically adjust exploration rate, search space and adaptation strategies.
    7.  Repeat steps 2 to 6 until the stopping criteria are met.
    8.  Return the identified threats and its respective solutions.
```

2.Performance Evaluation

In this section, an evaluation is carried out to test the efficacy of the proposed CDT-HS including communication overhead, energy consumption, detection rate, throughput, and latency. In a Multi-Layered V-IoT environment. The performance of the CDT-HS is evaluated against existing state-of-art methods like AES-RSA [14], GAPID [17], CVANET [18] and VCoT [20]. The proposed V-IoT is developed to ensure high-bandwidth and low-latent communication that supports faster data transmission between the IoT devices. The experimental setup is presented in Table 4, where the entire simulation is conducted in an NS-2.34 simulator that runs on an Intel i7 processor with 16GB of RAM.

Table 3: 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
CDT Parameters	
Splitting Criteria	Gini Impurity
Maximum Depth	10
Minimum Samples per Leaf	5
HS Parameters	
Population Size (N)	50
Dimension	2 (for latitude and longitude)

Splitting Criteria	Gini Impurity
Exploration Rate (*ER*)	0.1
Adaptation Rate (*AR*)	0.1
Maximum Iterations	1000
Latitude Range	-90 to 90 degrees
Longitude Range	-180 to 180 degrees
Initial Temperature	100
Cooling Rate	0.95

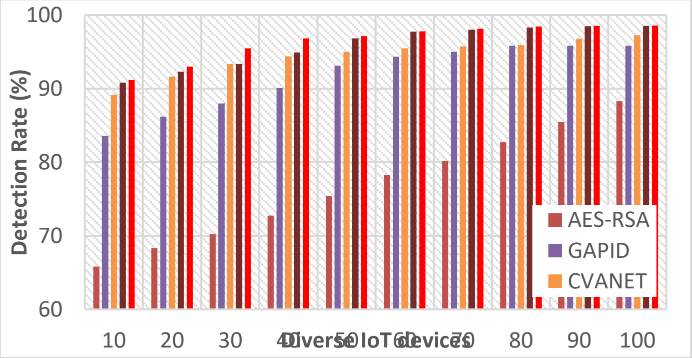

Figure 4: Detection Rate of different IoTs in VU in V-IoT environment

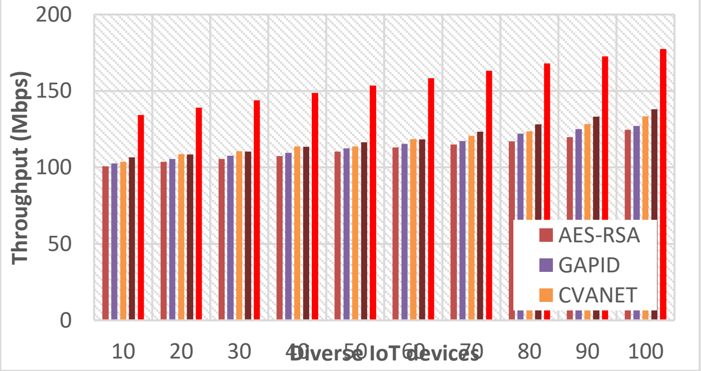

Figure 5: Throughput of different IoTs in VU in V-IoT environment

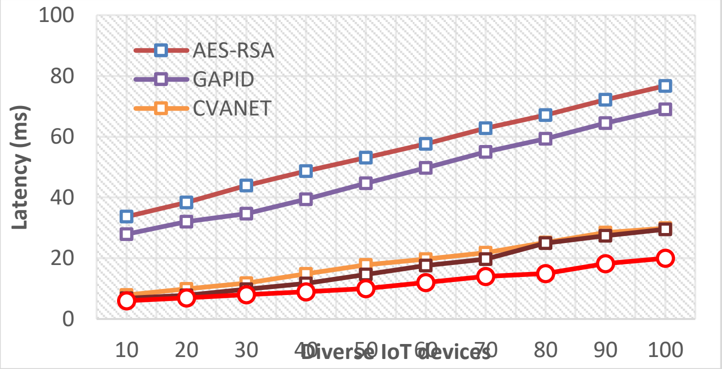

Figure 6: Latency of different IoTs in VU in V-IoT environment

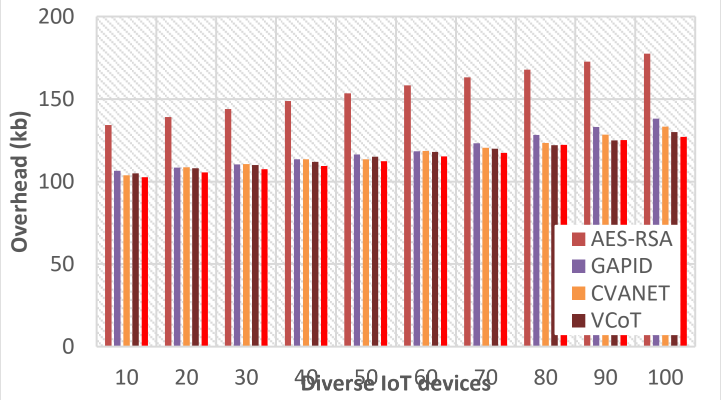

Figure 7: Communication Overhead of different IoTs in VU in V-IoT environment

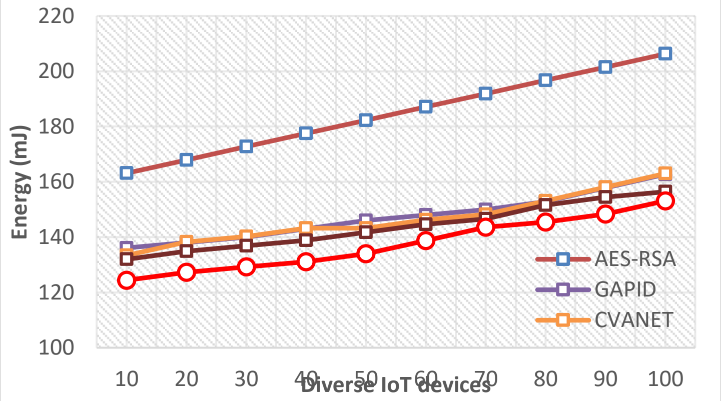

Figure 8: Energy Consumption of different IoTs in VU in V-IoT environment

The proposed CDT-HS outperforms other algorithms while detecting an attack as in Figure 4, where a significant improvement of 6.5% improvement is reported over VCoT. The proposed CDT-HS exhibits an improvement in throughput as in Figure 5 across various IoTs, where it outperforms other method by a desirable margin, with an average improvements of 2.7% over VCoT. The proposed CDT-HS achieves reduced latency compared to other algorithms, where a lower latency values of 8% reduction is achieved over VCoT as illustrated in Figure 6. The proposed CDT-HS outperforms other algorithms in terms of communication overhead as in Figure 7, where it achieves an 3% reduction than VCoT. Finally, the energy consumption is reduced across different IoTs in VUs, where a substantial margin of energy consumption of upto 1.7% is achieved over VCoT as in Figure 8.

3.Conclusion

The combination of CDT modeling and HS optimization contributes to an increased accuracy while authenticating the diverse IoT devices in VU. The careful selection of parameters like maximum depth and minimum samples per leaf aided in achieving increased detection rates. On other hand, the HS ability enables efficient exploration of the solution space to enhance the decision-making ability. The parallel data processing and quick authentication decision has improved the throughput rate, where parameters like initial temperature, and cooling rate influences the ability of HS to balance the exploration and exploitation, which leads to a better throughput. Thus, the optimization has further reduced the latency, communication overhead and energy consumption, which indicates the optimal settings in V-IoT environment.

References

1. Kumar, S., & Singh, J. (2020). Internet of Vehicles over VANETs: smart and secure communication using IoT. *Scalable Computing: Practice and Experience*, *21*(3), 425-440.
2. Twahirwa, E., Rwigema, J., & Datta, R. (2021). Design and deployment of vehicular internet of things for smart city applications. *Sustainability*, *14*(1), 176.
3. Islam, M. M., Nooruddin, S., Karray, F., & Muhammad, G. (2022). Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. *IEEE Internet of Things Journal*, *10*(4), 3611-3641.
4. Zhang, H., & Lu, X. (2020). Vehicle communication network in intelligent transportation system based on Internet of Things. *Computer Communications*, *160*, 799-806.
5. Hussain, R., Lee, J., & Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, *22*(5), 2553-2571.
6. Sultana, R., Grover, J., & Tripathi, M. (2021). Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges. *Vehicular Communications*, *27*, 100284.
7. Pourghebleh, B., Wakil, K., & Navimipour, N. J. (2019). A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet of Things Journal*, *6*(6), 9326-9337.
8. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201.
9. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3677.
10. Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A survey of IoT and blockchain integration: Security perspective. *IEEE Access*, *9*, 156114-156150.
11. Oktian, Y. E., Lee, S. G., & Lee, H. J. (2020). Hierarchical multi-blockchain architecture for scalable internet of things environment. *Electronics*, *9*(6), 1050.
12. Moura, J., & Hutchison, D. (2020). Fog computing systems: State of the art, research issues and future trends, with a focus on resilience. *Journal of Network and Computer Applications*, *169*, 102784.
13. Quyoom, A., Mir, A. A., & Sarwar, D. A. (2020). Security attacks and challenges of VANETs: a literature survey. *Journal of Multimedia Information System*, *7*(1), 45-54.
14. Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). A lightweight and secure online/offline cross-domain authentication scheme for VANET systems in Industrial IoT. *PeerJ Computer Science*, *7*, e714.
15. Chen, X., Yang, A., Tong, Y., Weng, J., Weng, J., & Li, T. (2022). A multisignature-based secure and OBU-friendly emergency reporting scheme in VANET. *IEEE Internet of Things Journal*, *9*(22), 23130-23141.
16. Goudarzi, S., Soleymani, S. A., Anisi, M. H., Azgomi, M. A., Movahedi, Z., Kama, N., ... & Khan, M. K. (2022). A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET. *Ad Hoc Networks*, *128*, 102782.

17. Raja, G., Anbalagan, S., Vijayaraghavan, G., Dhanasekaran, P., Al-Otaibi, Y. D., & Bashir, A. K. (2020). Energy-efficient end-to-end security for software-defined vehicular networks. *IEEE Transactions on Industrial Informatics*, *17*(8), 5730-5737.
18. Sharma, S., & Mohan, S. (2020). Cloud-based secured VANET with advanced resource management and IoV applications. *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*, 309-325.
19. Gnanajeyaraman, R., Arul, U., Michael, G., Selvakumar, A., Ramesh, S., & Manikandan, T. (2023). VANET security enhancement in cloud navigation with Internet of Things-based trust model in deep learning architecture. *Soft Computing*, 1-12.
20. Khattak, H. A., Farman, H., Jan, B., & Din, I. U. (2019). Toward integrating vehicular clouds with IoT for smart city services. *IEEE Network*, *33*(2), 65-71.