International Journal of Mathematical, Engineering and Management Sciences
Vol. 11, No. 1, 472-504, 2026
https://doi.org/10.33889/IJMEMS.2026.11.1.020

A Secured Data Delivery and Validation Model for Information-Centric Vehicular Cloud Network

Sanjeev Kumar Mekala
Department of Computer Science Engineering,
SRM University Andhra Pradesh, Neerukonda, 522502, Managalagiri, Andhra Pradesh, India.
E-mail: sanjeevkumar_mekala@srmap.edu.in

Satish Anamalamudi
Department of Computer Science Engineering,
SRM University Andhra Pradesh, Neerukonda, 522502, Managalagiri, Andhra Pradesh, India.
Corresponding author: satish.a@srmap.edu.in

Anil Carie Chettupally
Department of Computer Science Engineering,
SRM University Andhra Pradesh, Neerukonda, 522502, Managalagiri, Andhra Pradesh, India.
E-mail: anilcarie.c@srmap.edu.in

Murali Krishna Enduri
Department of Computer Science Engineering,
SRM University Andhra Pradesh, Neerukonda, 522502, Managalagiri, Andhra Pradesh, India.
E-mail: muralikrishna.e@srmap.edu.in

(Received on May 22, 2025; Revised on July 28, 2025 & September 17, 2025 & October 14, 2025;
Accepted on December 16, 2025)

Abstract

Road-safety data in Vehicular Ad Hoc Networks (VANETs) is becoming increasingly complex and diverse which leads to major challenges such as security flaws, ineffective data transmission, and risk of single-point failures. To address these issues, the Information-centric Vehicular Cloud (IVC) network has been adopted to secure data transactions. However, existing IV-based approaches still suffer from high latency and low Packet Delivery Ratio (PDR), which negatively impact the system performance. To overcome these limitations, the research proposed an efficient and secure data validation technique for VANETs. Vehicles generate various types of road safety data, which are transmitted to the destination via unicast forwarding. Caching vehicles are used to store frequently requested data to reduce latency and improve access speed. Also, a probabilistic data verification strategy is implemented, where vehicles verify transient data packets with a certain probability and exchange verification output to enhance accuracy. Each content provider signs the data and attaches verification metadata before transmission, which enables intermediate nodes to validate the content in transit. At the network edge, a Randomized Independent Verification Protocol (RIVP) with a Bloom filter is proposed to rapidly verify content authenticity, even when the complete verification information is embedded in the data itself. Experimental output illustrates that the proposed technique achieves a verification accuracy of 98.95% and a low verification overhead of 1.629%, which outperforms the existing method in terms of both security and efficiency.

Keywords- Road-safety data, VANET, Information-centric vehicular cloud, Verification protocol, Dataset generation.

Notation	**Description**
Dataset generation and forwarding	
RS_i	Road segment
vcn_i	IVC identifier
ds	Dataset
c_h	Vehicle

nc_j	Neighboring vehicle
t_{rp}	Time
u_d	Weight of the generated dataset
λ_d	Balancing coefficient ($0\leq \lambda_d \leq 1$) ()
v_d	Normalized resource weight
f_d	Normalized link weight
nc_a	All vehicles in the network
$v'(c_h, xc_j, vcn_i)$	Resource value nc_j for data delivery
$xw_h(vcn_i)$	Neighbor set of vehicles c_h
$xc_a \in xw_h(vcn_i)$	Resource value of any neighbor vehicle
$v'(c_h, xc_a, vcn_i)$	$xc_a \in xw_h(vcn_i)$ at the time t_{rp}
$f'(c_h, xc_j, vcn_i)$	Link duration between vehicles at the time t_{rp}
T_h	Start a timer
$cInt$	Interest packet
c'_h	Intermediate vehicle
$cData$	Caches data packet
$k'(vcn_i, t_{ca})$	Relative popularity of ds in vcn_i based on the number of times
P_i	Pending entry
g_i	Dataset lifetime
gn_i	Maximal lifespan of the dataset ds
tc_i	dataset ds generated time
$mc(vcn_i, t_{ca})$	A set of members caching the dataset ds at the time $mc(vcn_i, t_{ca})$
t_{ca}	Transaction time
$e'(vcn_i, t_{ca}, W_j)$	Catching member $W_j = mc(vcn_i, t_{ca})$
m_i	Overall caching weight
sc_i	Consumer
M_{Int}	request weight
λ_{RInt}, λ_{Zint}, and λ_{Qint}	balance coefficient
R_{Int}	Request Closeness
Z_{Int}	Request Intimacy
Q_{Int}	Request Centrality
$q(ds, xc_a)$	Distance from the vehicle $xc_a \in Y_h(ds)$ to RS_i
$q(ds, xc_j)$	Distance to RS_i
$b(ds, xc_a)$	The number of times that any vehicle encounter the member caching ds
$l(ds, xc_j)$	Frequency of vehicle xc_j meets other vehicles that are interested in ds
$l(ds, xc_a)$	Frequency of any vehicle $xc_a \in Y_h(ds)$ encounters other vehicles interested in ds
M_{data}	Response weight
λ_{Ld}, λ_{Zd}, and λ_{Rd}	Balance coefficients for response weight
L_{data}	Response Similarity
IT_h	Interest set of vehicle c_h
IT_i	Interest set of vehicles sc_i
$s(xc_a, sc_i)$	Number of times that any vehicle $xc_a \in Y_h(ds)$ encounter sc_i
R_{data}	Response Centrality
$y(xc_j, sc_i)$	Frequency of vehicle xc_j meets sc_i
$y(xc_a, sc_i)$	Frequency of $xc_a \in Y_h(ds)$ encounters sc_i
T_i	Timer that starts when the vehicle send a request for dataset

RIVP with bloom filter

$S_1, S_2, \ldots, S_n$	Set of intermediate nodes
S_1	First intermediate router
$R_1 = \frac{1}{n}$	The content with a probability
h	Position of router in the path
w	received content
λ	Number of hash functions used for insertion and querying
β	False Positive Rate
bloom	Bloom filter

Abbreviation	**Definition**
VANET	Vehicular Ad Hoc Networks
IVC	Information-centric Vehicular Cloud Network
PDR	Packet Delivery Ratio
RIVP	Randomized Independent Verification Protocol
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
ICN	Information-Centric Network
ICN-CoC	ICN-based Cooperative Caching
RFOP-VEC	Revocable access control scheme with Fair Incentive for Privacy-aware content delivery in Vehicular Edge Computing
BLAP-IOVs	Blockchain-based Lightweight Authentication Protocol
IoVs	Internet of Vehicles
PCC	Privacy-protecting Coded Caching framework
SRL	Swarm Reinforcement Learning
DRL	Deep Reinforcement Learning
ISCM	In-network Secure Content Management
SCD2	Secure Content Delivery and Deduplication scheme
SKP-ABE	Scalable Key-Policy Attribute-Based Encryption
CIFM	Collaborative Interest Forwarding Mechanism
FIB	Forwarding Information Base
PIT	Pending Interest Table
VIX	Vehicle-to-Infrastructure
RSU	Road Side Unit
CP	Content Provider
FPR	False Positive Rate
RIF	Router Information Filter
ECCN	Extended Content delivery solution for vehicular Content-centric Networking
FCCN	Data Delivery Framework for a vehicular content-centric network
IVC	Information-Centric Vehicular cloud
FNR	False negative rate

1. Introduction

VANET is growing as a significant development in the Internet of Things (IoT). The advanced modern technology for connecting sensors, network interfaces, and communication channels is VANET (Ahmed et al., 2024). These components can detect conditions and make smart decisions then share through wireless channels. The foundation of wireless communications has been the idea of Intelligent Transport Systems (ITS) (Mazhar et al., 2024). Roadside infrastructure and all forms of communication within and between cars are part of numerous communication scenarios. Vehicle-to-Vehicle (V2V) and Vehicle-to-

Infrastructure (V2I) communication are the two standard types of vehicular communication (Sajini et al., 2023). The development of Internet communication could be related to variations in the significance of content dissemination. Although continuous delivery, hop-by-hop, provides the basic structure of caching, there is an intimate interaction between system management and caching operations in the Information-Centric Network (ICN) (Ai et al., 2023; Bhardwaj et al., 2024). It is used to provide a communication system that is content-aware ensuring the network can intelligently conduct information activities including caching, dissemination, resolution, and preservation. Nowadays, the development of autonomous driving and wireless communication networks leads to improving the efficiency of automatic vehicles (Sangi et al., 2023; Sharma et al., 2024).

Some of the difficulties of ICN are unmetalled roads, highly congested city roads, inadequate road networks, poor bridge conditions, and so on (Lim, 2024). ICN may serve as a solution to the conflicts between the growing demands of users for content delivery and the current constrained bandwidth of IP networks. By using content identities instead of network addresses to find and retrieve content, ICN transfers the network's attention from the position of contents to user requests (Qaiser et al., 2025; Rizwan et al., 2023). The content-centric strategy known as ICN enables content to be accessed by storing and retrieving it using names. The accessibility of data in the network is increased by ICN, which also enables intermediate nodes to store material using effective caching mechanisms (Pruthvi et al., 2023; Wang and You, 2024). Every intermediate router can cache content and respond to user inquiries. Any local intermediate router uses the network's current resources, such as bandwidth and router cache space, to match user’s interests with content names and provide users with less latency content delivery (Ali et al., 2024). The ICN-based Cooperative Caching (ICN-CoC) technique was developed to select the cache by considering content attractiveness, rate prediction and cache position (Mahaveerakannan et al., 2024). A lightweight ICN content access control framework based on a hybrid coding mechanism was developed to reduce the complexity of ICN routers by integrating two or more encoding operations (Tan et al., 2023).

A novel Lightweight Blockchain-based Homomorphic Integrity and Authentication (Light-BHIA) scheme was developed to improve the privacy and integrity of content within ICNs (Chandra et al., 2025). A Revocable access control scheme with Fair incentives for Privacy-aware content delivery in Vehicular Edge Computing (RFOP-VEC) was developed to provide fair incentive distribution in privacy-aware data sharing. Here, a secure group signature scheme with formally proved security guarantees to enable anonymous authentication and conditional revocation (Jiang et al., 2024). A Blockchain-based Lightweight Authentication Protocol (BLAP-IOVs) was developed to ensure trustworthy Internet of Vehicles (IoVs) communication to achieve high success communication rates with acceptable V2V loss and computation overhead (Singh et al., 2024). A dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for VANETs was developed to overcome the anti-single-point failure, privacy preservation, and distributed security authentication of messages (Zhang et al., 2022). A Reputation Incentive Committee-based Secure Conditional Dual Authentication scheme (RIC-SDA) was developed to provide accelerated vehicle authentication. It integrates the dual authentication of consensus committee and V2V communication (Mahaveerakannan et al., 2024).

A Privacy-protecting Coded Caching framework (PCC) that ensures privacy has been developed for mobile ICNs. Here, the privacy protection quality evaluation model and the effective adversary model were developed to capture ICNs (Yang et al., 2023a). ICN is a unique technology that was examined to solve issues with content delivery. Research within the ICN framework aims to develop an internet structure that may replace the widely used existing IP-centric model (Hou et al., 2023; Qaiser et al., 2025). In order to deploy ICN for 5G communications, an Analytical method was created that uses a Dynamic (ICN-AD) population and based on various parameters such as user density, transmission speed, and the number of fixed nodes (Alsayaydeh et al., 2024). The Swarm Reinforcement Learning (SRL) was developed for a secured content caching mechanism which integrates salient features from both Swarm Learning (SL) and Deep Reinforcement Learning (DRL) (Yang et al., 2023b).

1.1 Problem Statement and Motivation

In VANETs, the higher complexity and variability of road safety data present significant challenges in terms of data reliability, communication efficiency and security. A major concern arises from the inability of a single vehicle to generate comprehensive data about surrounding environment, which leads to fragmented and incomplete safety information. In VANET, the latency and security remain critical challenges due to the high mobility of vehicles and dynamic network topology. Existing content verification mechanisms often depend on centralized or single-point verification, which introduces significant delays in authenticating safety-critical data before dissemination. These delays can cause in outdated or irrelevant safety alerts to reach vehicles too late to prevent accidents. Also, existing verification schemes lack efficient caching and probabilistic validation strategies, leading to network congestion and repeated verification overheads. Furthermore, dependency on a single content provider causes single-point failures, which makes the system vulnerable to disruptions or attacks. Unauthorized access during data transmission could cause tampering or loss of critical information. It compromises the effectiveness of real-time road safety applications. In recent years, several approaches have been developed in VANETs to strengthen data integrity and confidentiality with improved user privacy. Several data forwarding strategies have been introduced to optimize packet transmission with lower latency. However, despite these developed existing methods still face critical shortcomings including high verification latency, lower PDR, excessive communication overhead and limited scalability in dynamic vehicular environments.

To mitigate these issues, the IVC architecture was developed on the ICN framework, which has been adopted to facilitate collaborative data sharing among vehicles. However, this decentralized structure causes new challenges while reducing dependence on centralized nodes. Hence, the intermediate vehicles with caching capabilities can store and forward corrupted or unverified data, which undermines the reliability and consistency of overall system. These limitations necessitate a secure and efficient verification mechanism to ensure the authenticity of data in such a dynamic environment. Hence, the proposed model is developed to overcome these challenges by integrating probabilistic data validation and rapid verification using an RIVP with a bloom filter. It is utilized to ensure the secure content dissemination with low latency and high verification accuracy. The novelty of proposed model lies in its integration of a lightweight, probabilistic content verification mechanism within a decentralized IVC architecture for VANETs. Here, the RIVP with bloom filter is used to enable edge and intermediate vehicles to rapidly and efficiently verify the authenticity of content without requiring full access to validation at every node. The major contribution of the proposed technique is described as follows.

1) To enable rapid, lightweight and accurate validation of secured data in VANETs, the novel reification mechanism is developed using the Randomized Independent Verification Protocol (RIVP) with a bloom filter.
2) To improve the reliability of data validation, a probabilistic data verification approach is developed, enabling vehicles to independently validate transient data packets with a defined probability and share verification results to enhance overall trustworthiness.
3) To store and reuse frequently requested data, caching-enabled vehicles are used to reduce latency and improve PDR in a vehicular cloud environment.
4) To ensure secure and tamper-resistant content dissemination in decentralized IVC model, the intermediate nodes are used to validate content using attached signatures and verification metadata from content providers.

The remaining content of the paper is organized in the following manner: Section 2 includes a survey of existing techniques. In Section 3, the workflow and process of proposed methodology are described with figures. The security analysis of proposed model with varying attacks has been analysed in Section 4. The overall results are evaluated and discussed in Section 5 and the overall conclusion of the paper is given in Section 6.

2. Related Work

2.1 Literature Review

A survey of existing methods was reviewed and explained as follows.

2.1.1 Security and Trust Management in VANETs/ICN

A novel trust-aware VANET framework was developed by Bibi et al. (2024). Which integrates ICN and blockchain for content security. To ensure content integrity across the network, this method utilizes authenticated vehicle data to obtain efficient and effective security measures. It exhibits resilience against malicious assaults by improving throughput transactions and content delivery. The blockchain-based distributed security architecture was used to improve the security and provide reliable content delivery to the whole network.

A mechanism named In-network Secure Content Management (ISCM) was developed by Hlaing and Asaeda (2023). It used to enhance content integrity and authenticity in ICN using Identity-Based Cryptography (IBC) for content signature verification. To secure against tampering and illegal access to content, it utilizes a hybrid encryption-based access control method that ensures content confidentiality. ISCM provides scalable key distribution and secure content retrieval in ICN without significant amounts of communication delay or computing cost.

An anonymous protection mechanism was developed by Lu et al. (2023). To ensure secure content transmission from various sources to a consumer. The validity of various requested content forms from various anonymous content producers (sources) can be batch-verified by each anonymously authenticated content consumer. Assumes two-way authentication and consumer anonymity protection for ICN at same time.

A novel certification methodology for ICN was developed by Anisetti et al. (2022). Which supports continuous security verification of non-functional properties. It increases the trustworthiness of the network and its services by providing a full and detailed view of the network security state. This strategy expands upon an improved certification mechanism that documents the system's development over time. Also, it describes certification services that fully integrate with existing networks in order to collect data about the certification objective and finish the certification procedure.

A Secure Content Delivery and Deduplication scheme (SCD2) was developed by Xue et al. (2022). In ICN with various content providers, a Scalable Key-Policy Attribute-Based Encryption (SKP-ABE) scheme was developed to ensure efficient and secure fine-grained access control. This method simplifies key management by enabling fine-grained access control while enabling various attribute experts to share specific public attributes.

2.1.2 Forwarding Mechanism for Efficient Data Transmission

A V2R/V2V collaborative interest forwarding mechanism (CIFM) was introduced in Wang and Hou (2024) that makes the most of both communication paradigms and allows vehicles to switch communication modes according to the present network environment. Each node's interest packet forwarding was facilitated by a distinctive method.

A forwarding technique of interest packets was introduced in Qian et al. (2022) to reduce congestion by reducing network congestion. Shorter-distance nodes' data forwarding was carried out using this method. Those nodes were postponed and cancelled using an artificial delay.

2.1.3 Catching and Resource Optimization Strategies

An ICN-based energy-efficient content chunk placement was introduced in Gupta et al. (2023) by intercepting content copies on their route to the network edge router, the resource allocation strategy of this technique was used to decrease the content fetching delay. The EPC technique chooses where to store content chunks on each vehicle based on caching gain, local content popularity, and the residual power of the current vehicle. The EPC improves the effective use of network resources and decreases content duplication across the network by reducing chunk caching to vehicles whose residual power exceeds a threshold. The survey of existing techniques is described in **Table 1**.

Table 1. Survey of existing methods with their limitations and performance.

Author name and references	Year	Technique used	Limitation	Performance
Bibi et al. (2024)	2024	A trust-aware VANET framework	The security of data only depends on blockchain	It provides effective collaborations in ICN-based VANET communications
Hlaing and Asaeda (2023)	2023	ISCM	High content retrieval delay	Computational time – 80 ms
Lu et al. (2023)	2023	An anonymous protection mechanism	May occur Single point of failure	10 KB- communication overhead
Anisetti et al. (2022)	2022	A certification methodology for ICN	Limit its performance in dynamic environment	Average execution time 27 ms
Xue et al. (2022)	2022	SCD2 scheme	Limited storage resources	Response verification time – 2.694 ms
Al-Omaisi et al. (2024)	2024	GeoISA	Higher delay	67.8 % interest satisfaction rate (ISR) for 120 nodes
Qian et al. (2022)	2022	Forwarding strategy of interest packets	Mitigates congestion by intelligently postponing interest forwarding to reduce collisions	Postponement may delay critical packet delivery and affect real-time responsiveness
Gupta et al. (2023)	2022	An ICN-based energy-efficient placement of content	Effectiveness decreases when vehicle power is below the threshold	79 ms - content retrieval delay for 0.60 content popularity

2.2 Research Gap Analysis

Although various techniques have been developed to improve the VANET communication, existing models still face critical limitation which affects their performance, reliability and scalability. Bibi et al. (2024)'s ISCM suffers from high content retrieval delay, while Lu et al. (2023)'s anonymous protection mechanism risks single-point failure. Anisetti et al. (2022) developed a certification method for ICN which lacks adaptability in dynamic environments. Xue et al. (2022)'s SCD2 scheme was reduced by limited storage and slower verification. Al-Omaisi et al. (2024) reported higher delays with only 67.8% interest satisfaction rate. Qian et al. (2022)'s forwarding strategy reduces collisions but delays critical packet delivery. Gupta et al. (2023)'s energy-efficient ICN content placement loses effectiveness when vehicle power drops. These limitations emphasize the need for a more efficient, adaptive and secure ICN model.

3. Proposed Methodology

A single vehicle with limited capabilities can't generate comprehensive road-safety data. A single provider yields the data, resulting in a single point of failure; and any vehicle except the vehicle requester can access the data during data delivery leading to inefficient data communication. These issues are caused by the increasing complexity and variations in road-safety data in VANET. To overcome the limitations of VANET, the IVC is introduced. The members of IVC work together by sharing their resources to produce a dataset that includes various road safety data. Instead of using the network addresses of the contents, IVC locates and gets the contents using the ICN. Here, a data set can be transmitted by several vehicles. However, the previously mentioned benefits of IVC include fresh security risks. Unverified and corrupted contents have potential to be cached by vehicles and stay in the network throughout transmission since intermediate vehicles can separately select and cache elements during transmission. It concerns the legitimacy of content in the IVC network. To overcome this security problem, the proposed system leverages a Randomized independent verification protocol to protect content validity.

3.1 IVC-based VANET Network

The proposed system will adopts the V2V system model where VANET only consists of vehicles. Initially, the vehicles on each road segment will create a dataset with various types of road-safety data such as traffic, ice roads, etc. Then, unicast forwarding will be employed to deliver data sets to the destination. Here, the contents will be routed through two types of routers, namely RSU and Caching Vehicles. RSUs function as edge nodes that facilitate communication. Caching Vehicles are used to store previously requested data to reduce latency. In order to improve the verification process, they also share verification information and validate temporary data packets at a specific probability. Before the content is published, each Content Provider (CP) must authorize it and include extra verification details. This makes it easier for intermediate nodes to verify the content's authenticity. Edge nodes validate content sent by CP by using an RIVP with Bloom filter, despite whether the contents contain every detail required to verify the content's legitimacy. The architecture of IVC based on VANET network and the workflow of the proposed technique are represented in **Figures 1** and **2**.

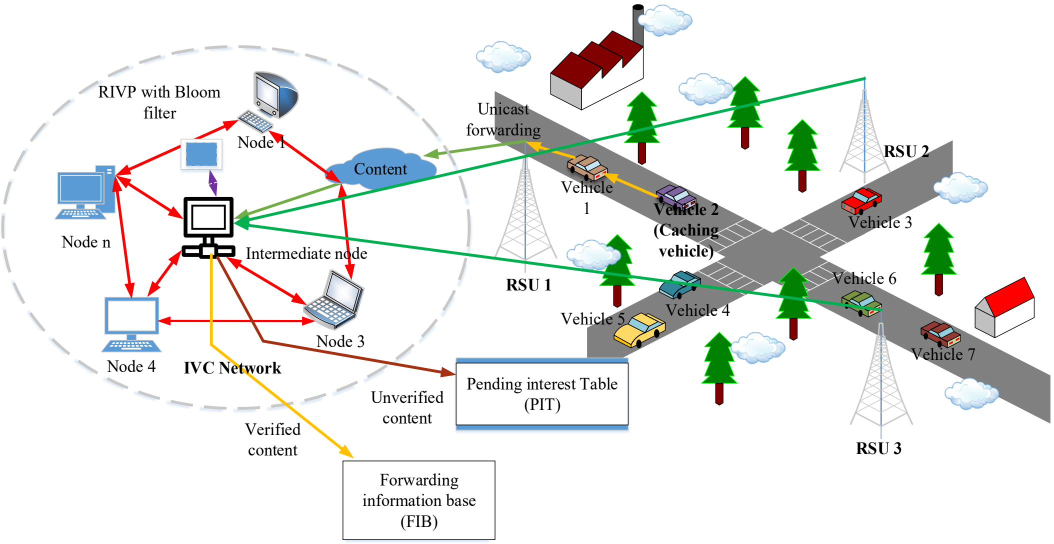


Figure 1. Architecture of IVC-based VANET network.

Figure 1 illustrates the architecture of an IVC-based VANET network integrating ICN for secure and efficient data delivery. On the left side, the IVC network comprises multiple nodes connected through intermediate routers that verify content using RIVP with bloom filters, which ensure efficient and probabilistic authentication of transmitted data. The Forwarding Information Base (FIB) stores routing information and verification status, while the Pending Interest Table (PIT) records unsatisfied interest packets to aggregate requests and guide data back to every consumers. On this right side, the vehicular network consists of vehicles communicating through RSUs. Vehicles send interest packets of dataset, which travel from content provider via RSUs using unicast forwarding. Verified data packets follow reverse paths guided by PIT entries.

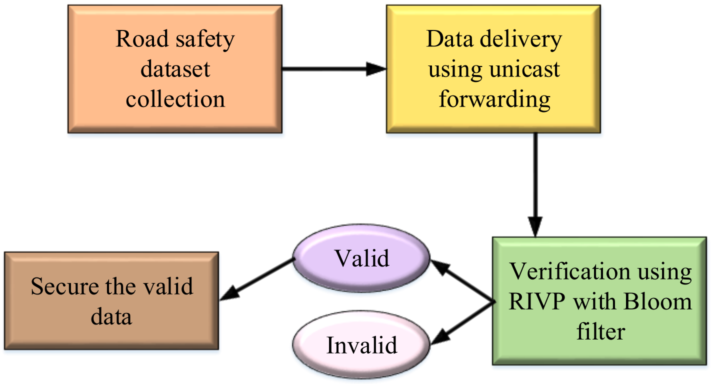

Road safety dataset collection
Data delivery using unicast forwarding
Verification using RIVP with Bloom filter
Valid
Invalid
Secure the valid data

Figure 2. Workflow of proposed methodology.

Figure 2 illustrates the proposed methodology for secure VANET data handling. Road safety datasets are collected and sent using unicast forwarding. Data is verified through RIVP with Bloom filters. Verified data is securely store while invalid data is discarded. It used to ensure the trusted, efficient and reliable vehicular communication and safety.

3.2 IVC Network

The VANET is used to establish V2I, Vehicle-to-Everything (V2X), and V2V communication. But, it suffers from security threats, data transmission delays and frequent disconnection due to high node mobility and network dynamics. ICN represents a paradigm evolution of communication from host-based to content-based. It employs unique content names to address data instead of IP addresses. This paradigm is suitable for highly dynamic environments such as VANETs because it offers name-based routing, content caching, and in-network data verification. Vehicle cloud computing and ICN are being highly incorporated through IVC. Vehicles are able to perform as caching/forwarding nodes along with data generators. The architecture enables reliability for inconsistent connectivity, redundancy reduction, and effective content delivery. Issues like content authentication, low PDR, and excessive latency remain despite its benefits.

3.3 IVC Dataset Delivery

The communication pattern of VANET is categorized into two types: V2V and V2I. The IVC generates and transmits real-time intervehicle datasets that are delay-sensitive and locally relevant. Autonomous vehicles can quickly exchange a real-time data set on neighboring vehicles, such as intervehicle distance and emergency braking systems, to facilitate safe driving. Generating intervehicle information is difficult for infrastructures due to the IVC dataset. Although vehicles require time and money to obtain real-time intervehicle information from infrastructures, the V2V model is used to develop and transmit IVC data sets. Hence, the V2V system is adopted by the proposed models, where VANET includes vehicles. This technique provides dataset generation, dataset caching and dataset delivery algorithm. Safe driving is made feasible by autonomous vehicles' ability to rapidly transmit real-time data on nearby vehicles, including intervehicle distance and emergency braking systems. The V2V model generates and provides IVC datasets because it is difficult for infrastructures such as RSUs to develop intervehicle information. Vehicles require time and money to obtain real-time intervehicle information from infrastructures.

3.3.1 IVC-based Dataset Generation

The challenge of generating a data set with different kinds of road safety data was not addressed by existing ICN-based solutions. Hence, the proposed IVC-based dataset generation algorithm is described in two folds.

(i) Since a name in an ICN is only linked to one type of data and is unable to identify a data set that includes multiple categories of data, the concept of a VCN is carried out to define a data set.

(ii) The vehicles can share resources and perform together to generate a data set due to a description of the IVC-based vehicle resource weight and intervehicle link weight.

The road segment labels are defined by VCN which includes several parameters regarding the road segment such as ice road, traffic, and so on. In the proposed IVC-based dataset generation algorithm, each road segment *RS$_i$* is labeled by IVC identifier *vcn$_i$* and the dataset *ds* for that segment comprises various road-safety parameters such as traffic, weather condition and road surface. The vehicle *c$_h$* responsible for generating *ds*, which selects a neighboring vehicle *nc$_j$* to deliver the dataset at time *t$_{rp}$* based on dataset generation weight *u$_d$*. It used to balances the resource capability and communication link stability of vehicles, which is given in Equation (1).

$$u_d = \lambda_d \cdot v_d + \left(1 - \lambda_d\right) \cdot f_d \tag{1}$$

Here, λ_d is a balancing coefficient ($0 \le \lambda_d \le 1$) which illustrates the relative importance of normalized resource weight *v$_d$* and the normalized link weight *f$_d$*. The resource weight *v$_d$* which is defined in Equation (2) to measure the storage and communication capability of *nc$_j$* compared to all vehicle *nc$_a$* in the neighbor set. Here, it evaluates the dataset *ds* transferred between normalized resource weights of vehicle *c$_h$* selecting vehicle *nc$_j$* at the time *t$_{rp}$*.

$$v_d = \frac{v'\left(c_h, xc_j, vcn_i\right) - \min_{xc_a} v'\left(c_h, xc_a, vcn_i\right)}{\max_{xc_a} v'\left(c_h, xc_a, vcn_i\right) - \min_{xc_a} v'\left(c_h, xc_a, vcn_i\right)} \tag{2}$$

Here, $v'\left(c_h, xc_j, vcn_i\right)$ is the resource value of *nc$_j$* for data delivery at *t$_{rp}$*. The neighbor set of vehicle *c$_h$* is represented as $xw_h\left(vcn_i\right)$at the time *t$_{rp}$*. Every vehicle in $xw_h\left(vcn_i\right)$ moves toward the road segment *RS$_i$* and the resource value of any neighbor vehicle $xc_a \in xw_h\left(vcn_i\right)$at the time *t$_{rp}$* is denoted as$v'\left(c_h, xc_a, vcn_i\right)$. Similarly, the normalized link weight *f$_d$* is described in Equation (3), which illustrates the reliability of the communication link between *c$_h$* and *nc$_j$*.

$$f_d = \frac{f'\left(c_h, xc_j, vcn_i\right), - \min_{xc_a} f'\left(c_h, xc_j, vcn_i\right)}{\max_{xc_a} f'\left(c_h, xc_j, vcn_i\right) - \min_{xc_a} f'\left(c_h, xc_j, vcn_i\right)} \tag{3}$$

Here, $f'\left(c_h, xc_j, vcn_i\right)$ is the link duration between vehicle *c$_h$* and vehicle *xc$_j$* at the time *t$_{rp}$*. Based on *u$_d$*, vehicle *c$_h$* sends an interest packet *cInt* with to the selected forwarder and starts a timer *T$_h$*. During this period, *c$_h$* receives and caches data packet *cData* with *vcn$_i$*. Once the timer expires, it compiles the collected data into *ds*. Intermediate vehicle c'_h receiving *cInt* either returns the data if they have the requested information$dl\left(vcn_i, c'_h\right)$, or if they are the designated target, generate the pending entry *P$_i$* and forward *cInt* to another neighbor in $xw(RS_i, c_{h'})$ with the highest u_d. Vehicles receiving *cData* forward it along to reverser path if a matching P_i exists, which ensure the reliable unicast forwarding. This cooperative mechanism developed by normalized resources and link weights which allows vehicles to share storage and communication resource efficiently to generate a comprehensive dataset *ds* for each road segment. It significantly improves the data delivery reliability and reduce the latency compared to standard ICN approaches. The algorithm of dataset generation is described in **Table 2**.

Table 2. Dataset generation.

```
Sub-algorithm 1: vehicle $c_h$
Step 1: Select forwarder vehicle
Step 2: Send creation interest packet cInt with $vcn_i$
Step 3: Start timer $T_h$
Step 4: while $T_h$ is running:
Step 5: if cData with $vcn_i$ is received:
Step 6: then stop timer and proceed
Step 7: end if
Step 8: end while
Step 9: Generate dataset ds

Sub-algorithm 2: vehicle $c'_h$ receiving cInt with $vcn_i$
Step 1: if data availability $dl(vcn_i, c_{h'})$ is true
Step 2: send creation data cData with $dl(vcn_i, c'_h)$
Step 3: end if
Step 4: if the current vehicle is the destination
Step 5: generate processing entity $P_i$
Step 6: if neighbor set $xw(RS_i, c'_h) \neq \phi$:
Step 7: select forwarder vehicle
Step 8: forward cInt to selected forwarder
Step 9: end if
Step 10: end if

Sub-algorithm 3: vehicle $c''_h$ obtaining cInt with $vcn_i$
Step 1: if processing entity $P_i$ is true
Step 2: forward cData to next hop.
Step 3: end if
```

Table 2 illustrates that the algorithm of dataset generation, which explains how the vehicular node in an IVC environment collaboratively generate and distribute a dataset *ds* based on the content request vcn_i. In subalgorithm 1, a vehicle c_h initiates that the process by selected an optimal forwarder vehicle. Then send a content interest packet *cInt* containing vcn_i and the starting a time to wait for the response. During this waiting period, if content *cData* with vcn_i is received before the timer expires, T_h terminates the wait and constructs the dataset *ds*. The subalgorithm 2 defines how a receiving vehicle c'_h handles an incoming *cInt*. If it already has the data attributes $dl(vcn_i, c'_h)$, it responds by sending *cData*. Else if it is the destination node, it generate a processing element P_i and if neighbor node $dl(vcn_i, c'_h)$ are available, selects the forwarder to relay *cInt*. Subalgorithm 3 manages a vehicle c''_h receiving *cData*; if P_i is valid, it forwards the *cData* further. This timer-based forwarding and responsive strategy ensure the dataset construction across vehicular network.

3.3.1.1 Dataset Details

The VANET traffic dataset used in this study was obtained from publicly available mobility and traffic trace repositories, which provide realistic large-scale dataset for simulating vehicular communication scenarios. The dataset was generated using a traffic simulation tool, such as data from Simulation of Urban Mobility (SUMO) integrated with real-world road network maps extracted from OpenStreetMap (OSM). Vehicle mobility traces were collected by modelling different traffic densities including low, medium and high traffic loads to emulate diverse urban and highway conditions. Each dataset entry includes key parameters such as vehicle ID, location coordinates, velocity, acceleration, inter-vehicle distance and road segment attributes (e.g., traffic congestion, road surface and weather conditions). The dataset also incorporates communication-specific metrics such as packet generation rate, transmission range and V2V link stability, which are crucial for evaluating VANET performance. These characteristics ensure that the dataset closely mirrors real-world vehicular environments, which makes it suitable for analyzing delay-sensitive, safety-critical data delivery in proposed IVC-based VANET framework.

3.3.2 IVC-based Dataset Caching

The proposed IVC-based dataset caching algorithm addresses the limitations of existing ICN caching, which is used to handle only single-type data by considering entire IVC-based dataset *ds*. This dataset *ds* includes diverse road-safety information. For each dataset *ds*, the caching decision at t_{ca} depends on three key attributes such as hit rate k_i, lifetime l_i and availability e_i, which are defined by a vehicular cloud network identifier vcn_i. The normalized hit rate k_i is defined by Equation (4), which is used to evaluate the relative popularity of *ds* in the VCN set vcn_i based on the number of times $k'\left(vcn_i, t_{ca}\right)$, it has been requested.

$$k_i = \frac{k'\left(vcn_i, t_{ca}\right) - \min_{vcn_j} k'\left(vcn_j, t_{ca}\right)}{\max_{vcn_j} k'\left(vcn_j, t_{ca}\right) - \min_{vcn_j} k'\left(vcn_j, t_{ca}\right)} \tag{4}$$

The dataset lifetime g_i is described by Equation (5), which measures how close *ds* is to expiration, where tc_i is its generation time and gn_i is its maximum valid lifespan.

$$g_i = \left(tc_i \_ gn_i - t_{ca}\right) \cdot gn_i^{-1} \tag{5}$$

Here, the dataset *ds* generated time is denoted as tc_i and the maximal lifespan of dataset *ds* is denoted as gn_i.

$$e_i = \sum_{W_j \in e'\left(vcn_i, t_{ca}\right)} \left(e'\left(vcn_i, t_{ca}, W_j\right)\right)^{-1} \tag{6}$$

Here, the set of members caching dataset *ds* at the time t_{ca} is denoted as $mc\left(vcn_i, t_{ca}\right)$ and the distance between the vehicles receiving dataset *ds* at the time t_{ca} and catching member $W_j = mc\left(vcn_i, t_{ca}\right)$ is denoted as $e'\left(vcn_i, t_{ca}, W_j\right)$. The datasets cached by more neighbor vehicles with higher e_i, which implying better availability. Finally, the overall caching weight m_i is defined in Equation (7) whether *ds* should be cached and evaluated as weighted combination of these attributes. It is performed based on Equations (4), (5) and (6).

$$m_i = \lambda_K \cdot k_i + \lambda_G \cdot g_i + \lambda_E \cdot e_i^{-1} \tag{7}$$

Here, λ_K, λ_G and λ_E is the balance coefficient for hit rate k_i, lifetime g_i and availability e_i, which can be tuned dynamically to emphasize dataset popularity, freshness or availability based on system priorities. Vehicle receiving *ds* at time t_{ca}, evaluate m_i and cache the data if the weight meets a predefined threshold, which ensures that requested and widely available datasets are prioritized for storage, reducing latency and improving data accessibility across the vehicular network.

3.3.3 IVC-based Dataset Delivery

A unicast forwarding is employed to deliver data sets to the destination. Here, the contents will be routed through two types of routers namely RSU and Caching Vehicles. RSUs function as edge nodes that facilitate communication. The failure of ICN-based delivery solutions to transmit an IVC-based dataset which includes various types of road safety data in a single data delivery process makes them ineffective in IVC. Also, the lack of efficient mobility support strategies causes frequent IVC-based dataset delivery failures. To overcome these kinds of issues, now the IVC-based dataset delivery algorithm has been developed two-fold which is described as follows.

- To avoid the dataset delivery issues caused by invalid FIB, the IVC-based request social attributes were created to route requests toward the best members.
- To avoid delivery failures caused by broken reverse paths and consumer mobility, the IVC-based response social attributes are generated for transferring the datasets to vehicle customers.

3.3.3.1 Request Social Attributes

The request social attributes need to avoid request delivery issues based on member mobility and enhance the delivery of requests to the best members. The process of requesting social attributes is performed based on threefolds, which are described as follows.

- Vehicles closer to target road segment frequently to meet member's caching target dataset.
- A vehicle meets members frequently; it is more likely to encounter them again.
- A vehicle meets other vehicles that are interested in target datasets, it is more liable to encounter members.

The request social attributes ensure that the interest packer *cInt* of consumer sc_i reaches optimal members caching ds. The request weight M_{Int} for vehicle c_h selecting neighbor xc_j is denoted in Equation (8).

$$M_{Int} = \lambda_{RInt} \cdot R_{Int} + \lambda_{ZInt} \cdot Z_{Int} + \lambda_{QInt} \cdot Q_{Int} \tag{8}$$

Equation (8) is used to forward a request for dataset *ds*, the request social-attribute weight M_{Int} of vehicle c_h. Here, λ_{RInt}, λ_{ZInt} and λ_{QInt} are represented as balance coefficient.

- **Request Closeness (R_{Int}):** It used to evaluate the proximity of xc_j to the target road segment RS_i using Equation (9).

$$R_{Int} = \frac{\max_{xc_a} q(ds, xc_a) - q(ds, xc_j)}{\max_{xc_a} q(ds, xc_a) - \min_{xc_a} q(ds, xc_a)} \tag{9}$$

Here, distance from the vehicle xc_j to road segment RS_i defined by vcn_i is denoted as $q(ds, xc_j)$. The distance from the vehicle $xc_a \in Y_h(ds)$ to road segment RS_i is denoted as $q(ds, xc_a)$.

- **Request Intimacy (Z_{Int}):** It normalize the number of times xc_j has encountered members caching *ds*, which is described in Equation (10).

$$Z_{Int} = \frac{b(ds, xc_j) - \min_{xc_a} b(xc_a)}{\max_{xc_a} b(xc_a) - \min_{xc_a} b(xc_a)} \tag{10}$$

Here, $q(ds, xc_j)$ is the encounter frequency. The number of times that any vehicles $xc_h \in Y_h(ds)$ encounter the member caching dataset *ds* is represented as $b(ds, xc_a)$.

- **Request Centrality (*Q_{Int}*):** It normalizes the frequency with *xc_j* meets other vehicles interested in *ds*, which is described in Equation (11).

$$Q_{Int} = \frac{l(ds, xc_j) - \min_{xc_s} b(ds, xc_a)}{\max_{xc_s} b(ds, xc_a) - \min_{xc_s} b(ds, xc_a)} \tag{11}$$

Here, the frequency of vehicle *xc_j* meets other vehicles interested in dataset *ds* is denoted as *$l(ds, xc_j)$* and the frequency of any vehicle $xc_a \in Y_h(ds)$ encounters other vehicles interested in dataset *ds* is denoted as *$l(ds, xc_a)$*.

3.3.3.2 Response Social Attributes

The response social attributes are used to transfer the dataset to vehicle customers and prevent response delivery failures caused by broken consumer mobility and reverse paths. The response social attributes are performed based on three folds which are described as follows.

- ❖ A vehicle's probability of transforming into a consumer increases with the degree of common interests between each other.
- ❖ A vehicle's probability of running into a customer again increases with the number of times it encounters them.
- ❖ The probability that a vehicle comes into contact with a customer increases with the frequency of those interactions.

Response social attributes ensure that *aData* reliably reaches the consumer *sc_i* to overcome mobility and broken reverse path. The response weight *M_{data}* is evaluated using the Equation (12).

$$M_{data} = \lambda_{Ld} \cdot L_{data} + \lambda_{Zd} \cdot Z_{data} + \lambda_{Rd} \cdot R_{data} \tag{12}$$

Here, the balance coefficients are represented as λ_{Ld}, λ_{Zd} and λ_{Rd}.

- **Response Similarity** (L_{data})**:** It utilize the jaccard coefficient of interest sets IT_j (of xc_j) and IT_i (of sc_i), which normalized among all neighbors xc_a and it is described in Equation (13).

$$Y_{data} = \frac{|IT_j \cap IT_i| \cdot (|IT_j \cap IT_i|)^{-1} - \min_{xc_a} |IT_a \cap IT_i| \cdot (|IT_a \cap IT_i|)^{-1}}{\max_{xc_a} |IT_a \cap IT_i| \cdot (|IT_a \cap IT_i|)^{-1} - \min_{xc_a} |IT_a \cap IT_i| \cdot (|IT_a \cap IT_i|)^{-1}} \tag{13}$$

Here, the interest set of vehicle c_h is denoted as IT_h and the interest set of vehicle sc_i is represented as IT_i and the interest set of any vehicle $xc_a \in Y_h(d_i)$ is denoted as IT_h.

- **Response Intimacy** (Z_{data})**:** It normalizes the number of encounters $s(xc_j, sc_i)$ between $xc_j \in Y_h(ds)$ and sc_i, which is described in Equation (14).

$$Z_{data} = \frac{s(xc_j, sc_i) - \min_{xc_a} s(xc_a, sc_i)}{\max_{xc_a} s(xc_a, sc_i) - \min_{xc_a} s(xc_a, sc_i)} \tag{14}$$

Here, the number of times that any vehicle $xc_a \in Y_h(ds)$ encounter consumer sc_i is represented as $s(xc_a, sc_i)$.

- **Response Centrality (R_{data}):** It normalizes the frequency of encounters $y(xc_j, sc_i)$, which is described in Equation (15).

$$R_{data} = \frac{y(xc_j, sc_i) - \min_{xc_a} y(xc_a, sc_i)}{\max_{xc_a} y(xc_a, sc_i) - \min_{xc_a} y(xc_a, sc_i)} \tag{15}$$

Here, the frequency of vehicle xc_j meets sc_i is denoted as $y(xc_j, sc_i)$ and the frequency of any vehicle $xc_a \in Y_h(ds)$ encounters the consumer sc_i is denoted as $y(xc_a, sc_i)$.

3.3.3.3 Social Attributes-based Dataset Delivery

In this paper, the social attribute-based dataset delivery technique utilized the advantage of dataset caching and social attributes to access dataset from optimal members in unicast. The *vcn*$_i$ defined the dataset *ds* fetched by vehicle consumer *sc*$_i$ based on dataset delivery algorithm which includes three subalgorithms.

- **Sub-algoirthm1 (Consumer Requesting data):** Consumer *sc*$_i$ selects the neighbor with the highest M_{Int}, which forwards with *vcn*$_i$ and waits for *sData* within timer T_i. Here, T_i represents a timer that starts when the vehicle consumer send a request for the dataset ds . Its initial value is set to be predefined timeout threshold configured by IVC framework based on expected network latency and average number of hops to reach a caching member. (The time reduces automatically with real-time progress, once it reaches zero. Then, it terminate and preserves an infinite wait). The purpose of while T_i loop is to allow the consumer to wait only within this bounded interval for incoming *sData*. If no data arrives before T_i expires, the process times out and the algorithm either retries with a different forwarder or aborts the request. Then, *sData* represents the actual safety dataset (response) that is transmitted after an interest request *sInt* is received. It includes the requested safety data send by caching vehicle back to the requesting vehicle. *sInt* represents an interest/request packet that a vehicle sends when it wants to retrieve specific safety-related data. It used to triggers the search process in caching-enabled vehicles. If a cache node has the requested data, it responds immediately. Otherwise, the interest packet is forwarded to the next eligible node.

- **Sub-algorithm2 (Forwarding Interest Packets):** Intermediate vehicle c_j checks its cache *ds*. If yes, it send *sData* using the neighbor with the highest M_{data}. If not and its neighbor set $xy_j(ds)$ is non-empty, it forward *sInt* based on *sInt*. Else, it carries the request until new neighbors are encountered.

- **Sub-algorithm3 (Data forwarding and caching):** After receiving, *sData*, vehicle decide whether to cache *sc*$_i$ based on caching weights, thus becoming members for future requests. Delivery continues toward *sc*$_i$ through neighbors with the highest M_{data}. The algorithm of dataset delivery based on social attributes is described in **Table 3**.

Table 3 illustrates the algorithm for dataset delivery which ensures the efficient retrieval and dissemination of an IVC-based set ds within the ICN framework using social attributes for optimal forwarding. In subalgorithm 1, vehicle consumer *xc*$_i$ initiates a request by selecting the neighbor with highest required weight, sending an interest packet *sInt* carrying *vcn*$_i$ and starting a timer. If *sData* containing ds arrives before the time expires, the data is cached locally and process terminates. Subalgorithm 2 govern how the intermediate c_j processes *sInt*. If *ds* is cached, then it replies with *sData*, else forwards the request to neighbors with higher request weights or carries it until new neighbor appears. Subalgorithm 3 handle the data reception, where c_j may cache ds based on caching weight and become a new provider. If the destination is reached, it *sData* is forwarded along optimal paths and ensures lower delay and robust data delivery. Else it continues forwarding toward the next hop and ensures the reliable delivery.

Table 3. Algorithm of dataset delivery.

```
Sub-algorithm 1: vehicle consume $xc_j$
Step 1: Select the forwarder vehicle
Step 2: Send the request packet sInt with $vcn_i$
Step 3: Start timer $T_i$
Step 4: while $T_i$ is running
    Step 5: if a response packet sData with ds is received
        Step 6: cache ds
    Step 7: end if
Step 8: end while
Step 9: return (terminate the sub-algorithm 1)
```

```
Sub-algorithm 2: vehicle $c_j$ receiving sInt with $vcn_i$
Step 1: if ds is cached locally:
    Step 2: Send sInt with $vcn_i$
    Step 3: return (terminate sub-algorithm 2).
Step 4: end if
Step 5: if $c_j$ is the destination:
    Step 6: if neighbor set $xy_j(ds) = \phi$:
        Step 7: Select next-hop forwarder
        Step 8: forward sInt to selected forwarder.
    Step 9: else
        Step 10: transfer sInt until encounter new neighbours
    Step 11: end if
Step 12: end if
Step 13: repeat until ds is successfully delivered
```

```
Sub-algorithm 3: vehicle $c'_j$ receiving sData with ds
Step 1: if cache decision allows caching ds:
    Step 2: cache ds and become member node.
Step 3: end if
Step 4: if $c'_j$ is the destination:
    Step 5: if neighbor set $xy'_j(ds) = \varphi$
        Step 6: Select next-hop forwarder
        Step 7: forward sData to the next hop
    Step 8: else
        Step 9: transfer sData until encounter new neighbours
    Step 10: end if
Step 11: end if
Step 12: repeat until ds is successfully delivered
```

3.4 Authentication Process using RIVP with Bloom Filter

If a CP releases unverified content that enters the network via an edge router, the ICN network selects an intermediary router to verify the content using a RIVP. The purpose is to reduce redundant verification and overhead by ensuring that every content of content is certified precisely once by a minimum of one router. Intermediate routers have a Bloom filter in place to allow rapid authentication, preserving verification results from other routers as well as from their own tests for future reference. The two methods used in the following two subsections are described as follows.

3.4.1 RIVP

In this scheme, every intermediate router based on content path cooperative to process RIVP verification to ensure that at least one router verifies the content. Consider n as the number of hops (intermediate routers) between CP and user, which were reordered in the interest packet. The set of router is $S_1, S_2, ..., S_n$, where S_1 is the first intermediate router. The first router S_1 verifies the content with a probability $R_1 = \frac{1}{n}$. If the content is confirmed valid, then it is marked with valid label and all subsequent routers forward it without further analysis. If S_1 skips verifications, the responsibility passes to S_h which now verifies the content with a re-evaluated probability, which is described in Equation (16).

$$S_h = \frac{1}{n-(h-1)} \tag{16}$$

Here, h is the position of the router in the path. The Equation (16) is used to ensure that every router have an equal chance of verifying the content. According to the probabilistic verification setup, P (verify at router h) is equal to S_h, which stands for the verification probability for the h^{th} router. In order to preserve an equal selection probability across all routers, both representations guarantee that precisely one router completes verification. The sum of probabilities across routers which ensures exactly one verification before the content reaches the user.

Each router executes the *verify*(w) function, where w is the received content. If the verification is performed and the content is valid, then the router adds the output to its bloom filter. Later request for same content can be rapidly authenticated by checking the bloom filter, which avoiding repeated computation. If no previous router has verified content, subsequent routers continue the probabilistic verification process based on Equation (16).

In ICN, multiple users often request the same content simultaneously. In order to reduce redundant transmission, the router aggregates requests for identical content when many interest packets arrive at the same intermediate router. The router saves all subsequent similar interest packets in the PIT after forwarding the first one that eventually occurs. The PIT retains the information about incoming interfaces, interest names and metadata, which allows the router to forward the eventual data packet to every requesting user without reissuing multiple upstream interests. Once the CP sends the requested content, it passes to the aggregation router that utilizes PIT to transfer the data individually to every requesting user. The FIB assists in forwarding by maintaining a mapping between the content prefixes and next-hop interfaces. Now, it also incorporates the verification status flags which indicate whether the RIVP has been applied to secure the content path.

During this process, every router along the original interest packet pathway participates in this probabilistic verification to ensure that content is authenticated exactly once. The verification probability S_h is reassessed for routers in the path between a single router and the relevant user if previous router did not validate the content. By integrating the PIT-based request aggregation, FIB-based interest forward and Bloom filter-based probabilistic verification, this proposed mechanism reduces duplicate processing and effectively handles multiple interest packets. It ensures the content integrity while delivering the verified content to every consumer. The algorithm of RIVP for verification is described in **Table 4**.

Table 4 illustrates that the RIVP algorithm ensures secure content verification in a probabilistic manner. Given content w, verification mark *mark* and number of participating router h, initially it verifies if *mark* indicates validity. If so, w is forwarded without further verification. Else, the router evaluates the verification probability using Equation (16) and probabilistically decides whether to verify. If verification succeeds *verify*(w), the content is marked valid and forwarded. If verification fails, w is dropped and the router re-analyzes the content with *mark* from edge router and resends interest request if required. It ensures balanced verification and reduced overhead in IVC.

Table 4. Algorithm of RIVP.

```
Input: verify the content, $w$
The mart from content’s intermediate router $mark$
Number of participating routers $h$

Step 1: if $mark$ is valid then
Step 2:     forward the content $w$ without verification
Step 3: end
Step 4: else
Step 5:     evaluate probability to verify the content using Equation (16)
Step 6:         whether the probabilistic choice to verify the content
Step 7:     if $choice$ to verify then
Step 8:         if $verify(w)$ then
Step 9:             mark the content $w$ is valid
Step 10:            forward the content $w$
Step 11:        end
Step 12:        else
Step 13:            drop $w$
Step 14:            analyze the content $w$ with mark from edge router
Step 15:            resend the content interest with its name
Step 16:        end
Step 17:    end
Step 18: end
```

3.4.2 Verification and Data Sharing through Bloom Filter

Bloom filters are used by the intermediate routers in ICN network for fast verification of content authenticity and to share verification results among routers. The process consists of four stage: Initialization of bloom filter, verification, share verification data with bloom filter and update the bloom filter. The bloom filter's initial setup, the application and sharing of authentication information based on it, which is described as follows.

3.4.2.1 Bloom filter Initialization

Every intermediate router may initiate bloom filter *bloom* using the operation $bloom \leftarrow bf.setup(w, \lambda)$, where filter size (number of bits) is denoted as w and the number of hash functions used for insertion and querying is denoted as λ. To ensure significant efficacy, the ISP specifies an upper bound on False Positive Rate (FPR) β (probability that filter incorrectly marks the unverified content as valid). The selection of initial situations such as β, λ and w depends on the network's size and each router's traffic load to balance the storage efficiency and accuracy.

3.4.2.2 Verification Process

Content is validated and identified by a suitable tag, and the content title, along with its hash value is retained in a bloom filter. To verify content, an intermediate router verifies to determine when content is included within its bloom filters. The intermediate router can rapidly recognize validated content by using $test(bloom, x_w)$for hash lookup as a bloom filter, which logs each verified hash value of content to indicate that the content has been verified as valid. Otherwise, content must be validated using signature verification and, it has no matching signature or hash verification, it remains in the bloom filter. The signature in content with $verify\left(c_{h_i}, s_w, H(w)\right)$ verified by the intermediation router. Then, signature of valid content is included into *bloom* by using the defined operator $insert\left(bloom, x_w\right)$.

3.4.2.3 Share Verification Data

Routers frequently share *bloom* and every intermediate router will share the data when the sharing period is established by the ISP which is currently using and continuously updating to its neighboring routers. A router utilize OR (v) operation to merge the bloom filter with its bits to combine the various bloom filters when it receives a *bloom* from another router. Consider two bloom filters waiting to combine $bloom_1$ and $bloom_2$ to obtain $bloom = bloom \vee bloom_2$, which is verified as follows.

$$\forall \beta \in bloom_1 \rightarrow \beta \in bloom \tag{17}$$

$$\forall \beta \in bloom_2 \rightarrow \beta \in bloom \tag{18}$$

The router has to update the *bloom* when every single *bloom* reaches or exceeds the upper bound of the FPR.

3.4.2.4 Update Bloom Filter

The FPR of the aggregated bloom filter gradually improves when the various store signatures increase. Then, the new bloom filter will be obtained to ensure accuracy when the FPR of the bloom filter reaches the preset threshold. Also, the router will retain the outdated bloom filter. The intermediate node will initially retrieve the signature from the active bloom filter when it receives new data. It examines every stored old bloom filter in order of earliest to newest if there is no match. The node can be removed from historical bloom filters that have been kept for too long. The algorithm of verification of the RIVP with a bloom filter is described in **Table 5**.

Table 5. Algorithm for the process of verification with Bloom filter.

```
Input; unverified content $w$
Signature of content $w$, $x_w$
Public key of content
Bloom filter verification $Bloom$
Mark from the content's intermediate router $mark$

Step 1: if $test(Bloom, x_w)$ then
Step 2:     mark the content as valid
Step 3:     return valid
Step 4: end
Step 5: else
Step 6:     if $verify(c_{h_i}, s_w, H(w))$ then
Step 7:             $insert(bloom, x_w)$
Step 8:             return valid
Step 9:     end
Step 10:    else
Step 11:            return invalid
Step 12:    end
Step 13: end

Output:  valid or invalid
```

Table 5 illustrates the algorithm of the verification process with bloom filter. Given content *w*, its signature x_w, a public key and a verification mark, initially the system checks if x_w exists in bloom filter via $test\left(Bloom, x_w\right)$. If it is verified, the content is marked as valid. Otherwise, full signature verification

$verify\left(c_{h_i}, s_w, H(w)\right)$ is performed. Valid signatures are inserted into bloom filter for further verification. Here, the invalid content is rejected to ensure reliable and efficient authentication. The architecture and Flowchart of RIVP with Bloom filter are represented in **Figures 3** and **4**.

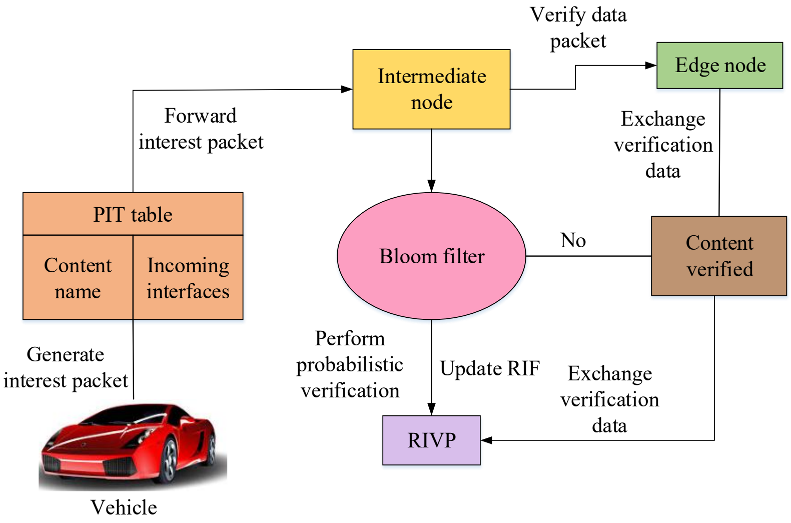


Figure 3. Architecture of RIVP with bloom filter.

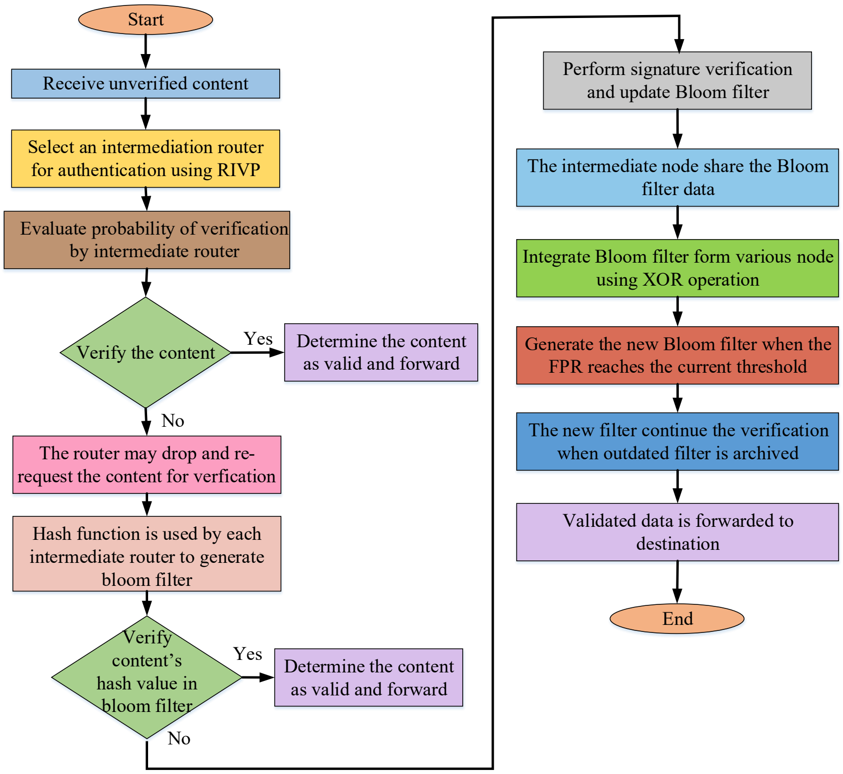

Start
Receive unverified content
Select an intermediation router for authentication using RIVP
Evaluate probability of verification by intermediate router
Verify the content
Yes
Determine the content as valid and forward
No
The router may drop and re-request the content for verfication
Hash function is used by each intermediate router to generate bloom filter
Verify content's hash value in bloom filter
Yes
Determine the content as valid and forward
No
Perform signature verification and update Bloom filter
The intermediate node share the Bloom filter data
Integrate Bloom filter form various node using XOR operation
Generate the new Bloom filter when the FPR reaches the current threshold
The new filter continue the verification when outdated filter is archived
Validated data is forwarded to destination
End

Figure 4. Flowchart of RIVP with bloom filter.

Figure 3 illustrates the architecture of RIVP integrated with a bloom filter for efficient data validation in an IVC-based ICN. This process starts with a vehicle generating an interest packet, which is recorded in PIT and stores the content name and incoming interfaces. This interest packet is forwarded to an intermediate node, where verification of the returning data packet occurs. The bloom filter is used for rapid authentication. If the content exists in the filter, it is immediately marked as verified. Otherwise, the RIVP performs the probabilistic verification, updates the Router Information Filter (RIF) and exchanges verification data with neighboring nodes to reduce redundancy. When verification succeeds, the data is marked as verified content and shared across the network.

Figure 4 represents the content authentication workflow using RIVP with bloom filter. The process begins when the unverified content enters the network. But the input is not explicitly marked with a proper starting symbol and make the entry point unclear. Then, the content is routed to an intermediate router, where the probability of verification is assessed under RIVP. If verified, the content is marked as valid and forwarded is missing and reducing the clarity. When verification fails, the router re-request the content or generate a bloom filter entry using a hash function. Then, the bloom filter checks if the content's hash exists. If so, it is validated and forwarded.

4. Security Analysis

The security analysis of proposed model for varying types of attacks is described as follows.

4.1 Content Forgery Attack

The proposed model utilized the RIVP with Bloom filter-based validation to detect and reject forged or tampered data. Verified signatures are stored in bloom filter and ensure only authenticated content transmission. The forged packet fail verification, preventing unauthorized data from propagating through the network and ensure trustworthy content delivery.

4.2 Replay Attack

Replay attempts are mitigated through verification marks and time-sensitive bloom filter entries. Each data packet carries a unique mark verified by intermediate routers. Replayed packets without valid verification marks are rejected. It prevents attackers from reusing old, legitimate packets to disrupt communication or mislead users.

4.3 Interest Flooding Attack

PITs aggregate the multiple identical requests to limit the number of interest packets forwarded. This reduced unnecessary network traffic, mitigating the effect of flooding attacks. Legitimate requests are still processed efficiently and ensure that malicious interest floods cannot overwhelm the router or degrade service availability.

4.4 Single-point Failure Attack

RIVP distributes probabilistic verification across multiple routers and eliminating dependency on any single node. This decentralized verification structure ensures that failure or compromise of one router does not disrupt the entire network. It significantly enhancing fault tolerance and maintains consistent performance during targeted attack or node failures.

4.5 Cache Poisoning Attack

The router utilized a bloom filter validation to confirm data integrity before caching. Malicious or tampered data that fails verification is immediately discarded and protects caches from pollution. It ensures that only authentic content is stored and prevents the spread of poisoned data and maintaining reliable, trusted content delivery across the network.

4.6 Man-in-the-Middle (MITM) Attack

Every transmitted content undergoes signature verification with stored hash values which makes undetected tempering nearly impossible. Attackers intercepting data cannot modify or inject malicious content without failed verification. Probabilistic multi-router checks further strengthen security, which ensure data integrity and protect end-users from malicious alterations during transmission.

4.7 Collusion Attack

Routers periodically share and merge bloom filters using XOR operation, decentralized verification and reducing the risk of colluding nodes bypassing verification. Even if some node integrates maliciously, other independent routers can still detect invalid data, which ensure consistent content integrity and reduce the vulnerabilities to coordinated internal attacks.

5. Results and Discussion

The performance of the proposed technique is compared with various existing techniques named extended content delivery solution for vehicular content-centric networking (ECCN), data delivery framework for a vehicular content-centric network (FCCN), and standard information-centric vehicular cloud (IVC) to determine its efficiency. In this research, the simulation setup has been elaborated to ensure transparency and reproducibility. This proposed model is evaluated in a VANET simulation environment using realistic dataset and the details. The simulation parameters and hyperparameter details of proposed model are represented in **Tables 6** and **7**.

Table 6. Simulation parameter details for proposed model.

Parameters	Description/Value
Simulation tool	NS-3 integrated with SUMO for mobility modelling
Dataset	Realistic VANET traffic traces with road safety data
Simulation duration	1000 seconds
Simulation area	1000 m x 1000 m
Number of vehicles	500
Vehicle speed range	10-30 m/s
Communication range	300 m
Data packet size	512 bytes
Bloom filter size	1024 bits
Hash function	4
PIT size	200 entries
FIB entries	500 entries
Interest generation rate	10 packets/sec
Number of hops	3-7

Table 7. Hyperparameter details of proposed methodology.

Hyperparameter	Values
Learning rate	0.001
Optimizer	Adam
Batch size	32
Dropout size	0.3
Epochs	300
Activation function	ReLU
Loss function	Cross-entropy
Feature dimension	256

A learning of 0.001 was selected as it provides a good balance between convergence speed and model stability. Higher values lead to divergence, while lower values slow convergence. The dropout rate of 0.3 was selected to effectively prevent overfitting while preserving sufficient network capacity for feature learning. A batch size of 32 was used to maintain computational efficiency without sacrificing gradient stability. The Adam optimizer was adopted due to its adaptive learning rate capability, which accelerates the convergence. Also, 300 epochs ensured that the proposed model had sufficient iterations to converge, while early stopping was monitored to avoid unnecessary overtraining. The Cache Hit Ratio in an ICN scenario is usually evaluated and represented using the following Sample Hit Ratio, which is described in **Table 8**.

Table 8. Hit ratio for ICN.

Number of vehicles (Nodes)	Cache size (MB)	Content request rate (req/sec)	Hit ratio (%)	Average latency (ms)
50	100	9	77.45	44.9
100	100	13	83.21	40.2
150	200	20	91.01	36.2
200	300	24	92.40	32.8
250	400	31	94.92	32.3
300	500	36	95.21	28.2

5.1 Performance Metrics and their Formulation

The performance of proposed technique is evaluated based on various metrics such as verification accuracy, verification overhead, FPR, false negative rate (FNR), end-to-end latency, PDR and content authenticity rate as described in **Table 9**.

Table 9. Performance metrics with its description and formulation.

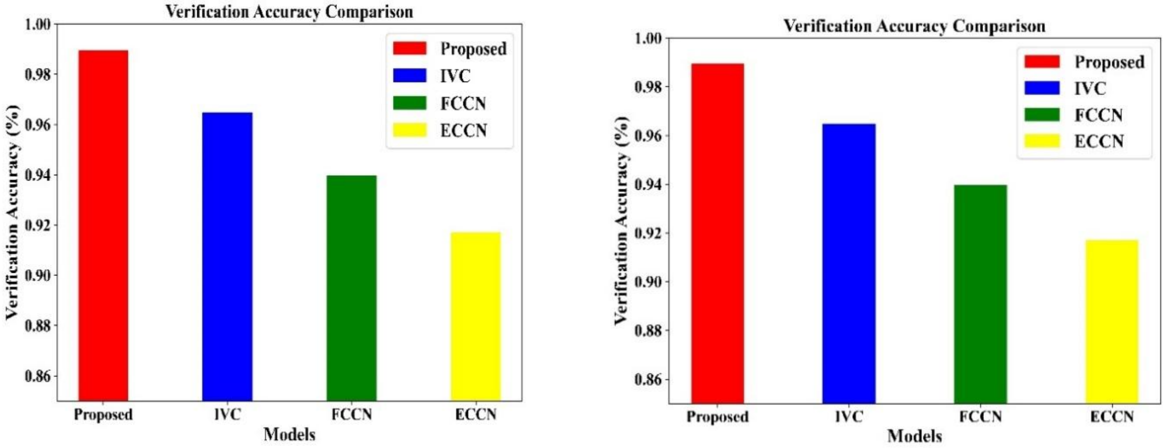
Performance metrics	Description	Formulation
Verification accuracy	It evaluates how effectively the model correctly detects the valid and invalid content	$VA = \frac{tp + tn}{tp + tn + fp + fn} \times 100$
Verification overhead	It evaluates the computation resource before forwarding the data in the network for validation	$OH = \frac{VT}{t} \times 100$
FPR	It evaluates how often invalid data is incorrectly identified as valid data	$FPR = 100 \times \frac{fp}{fp + tn}$
FNR	It evaluates how often the valid data is incorrectly identified as invalid and rejected	$FNR = \frac{fn}{fn + tp} \times 100$
PDR	It evaluates the percentage of successfully delivered packets over total transmitted packets in network	$PDR = \frac{RP}{SP} \times 100$
End-to-End Latency	It evaluates the total time required for data transmission from content provider to requestor (including verification and forwarding delays)	$Lat = RT + PT + VT$
Content Authenticity Rate	It evaluates the proportion of received data that passes through the validation checks and is determined as valid	$CAR = \frac{NV}{NV + NI} \times 100$

Here, the verification overhead is denoted as *OH*, the time required for verification and the total amount time consumed for data transmission are represented as *VT* and *t*. The true positive and true negative are represented as *TP* and *TN*. The FPR and false negative are represented as *FP* and *FN*. The content authenticity rate is denoted as *CAR*, the total number of valid data and number invalid data are represented as *NV* and *NI*. The end-to-end latency and transaction delay are represented as *Lat* and *RT*. The propagation delay and verification delay are represented as *PT* and *VT*. Various successfully received packets and total number of packets sent are represented as *RP* and *SP*.

5.2 Performance Analysis

The comparison of verification accuracy and verification overhead is represented in **Figure 5**.

The proposed technique achieves 98.95% verification accuracy and 1.629% verification overhead. The proposed technique attains higher verification accuracy and lower verification overhead compared to the other existing models. Edge nodes and caching vehicles can efficiently authenticate content using stochastic verification according to the proposed technique, which improves verification accuracy by utilizing an RIVP with a Bloom Filter. It reduces redundant computations, ensuring effective validation with low verification overhead and enhanced security by transferring verification information between nodes and selectively validating transitory packets. The comparison of FPR and FNR for both proposed and existing techniques is represented in **Figure 6**.



(a)

(b)

Figure 5. Comparison of (a) Verification accuracy and (b) Verification overhead.

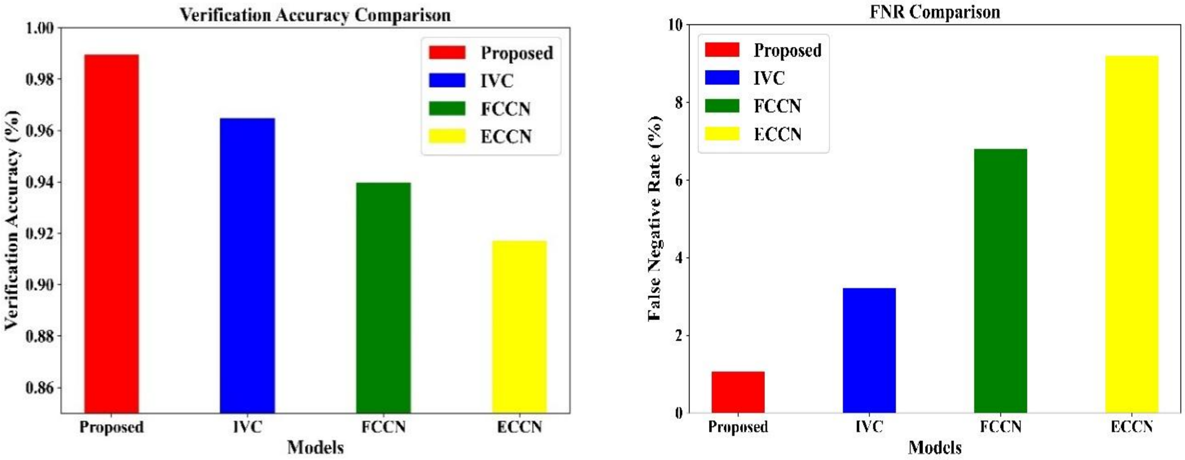


Figure 6. Comparison of (a) FPR and (b) FNR.

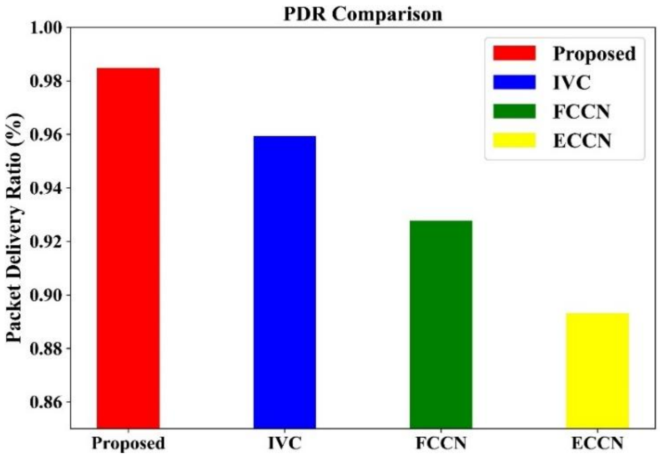


Figure 7. Comparison of PDR for proposed and existing techniques.

The FPR and FNR rates of the proposed technique are obtained to be 1.064% and 0.894%, which are lower than other existing techniques. The proposed approach reduces misclassification errors by using a Bloom filter for stochastic content verification, which lowers the FPR and FNR. RIVP improves accuracy by cross-checking recently received and cached data, substantially reducing false verifications by ensuring that only valid content is stored and transmitted. The comparison of PDR for proposed and existing technique is represented in **Figure 7**.

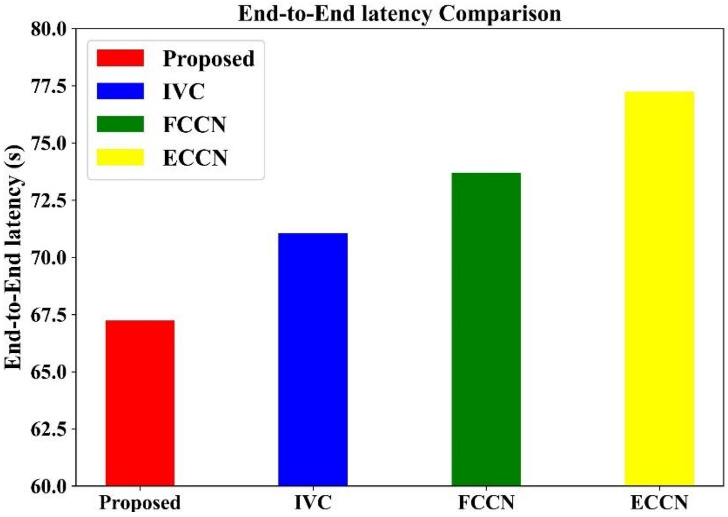


Figure 8. Comparison of End-to-End latency for proposed and existing techniques.

The PDR of proposed technique is obtained to be 98.48% accuracy which is higher than other existing techniques. The proposed approach utilizes caching vehicles and RSUs for effective data distribution, which enhances PDR. Retransmission of invalid packets is reduced by the Bloom filter-based verification, which ensures that only valid data is transmitted. Unicast forwarding ensures reliable data transmission to the intended receivers while minimizing congestion and improving network efficiency. The comparison of End-to-End latency for proposed and existing techniques is represented in **Figure 8**.

The proposed technique achieves 67.24s End-to-End latency, which is lower than other existing models. The proposed approach reduces duplicate transmissions and lowers end-to-end latency by using caching vehicles to store and efficiently retrieve frequently requested data. Unicast forwarding improves routing efficiency while content validation is accelerated by Bloom filter-based verification. The proposed model reduces processing time, network overload, and data delivery delays across VANET.

Although the measured end-to-end latency of 67.24 seconds may appear relatively high for standard VANET scenarios, it is important to note this value represents the cumulative latency of the complete end-to-end process including dataset generation, caching, forwarding and delivery across multiple hops rather than only the transmission delay of safety-critical messages. In practice, time-sensitive alerts such as collision warning or emergency braking signals are transmitted through prioritized control channels with significantly lower delays, while the reported latency pertains mainly to the transfer of the aggregated inter-vehicle dataset used for traffic management, road condition and long-term safety analysis. Hence, this latency is acceptable and it does not hinder the immediate decision-making of autonomous vehicles but instead ensures the reliable sharing of comprehensive vehicular datasets that support situational awareness, predictive modelling and network resilience in safety-critical applications.

The comparison of content authentication rates for proposed and existing techniques is represented in **Figure 9**.

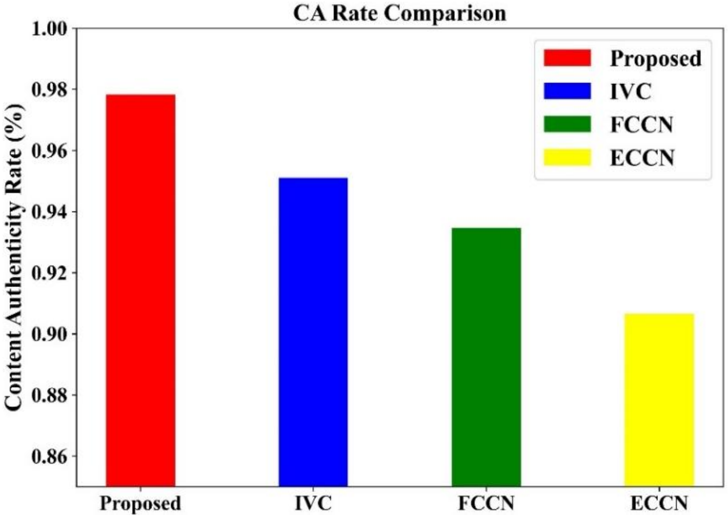


Figure 9. Comparison of content authenticity rate for proposed and existing techniques.

The proposed technique achieves a 97.83% content authentication rate which is higher than other existing techniques. By integrating Bloom filter with an RIVP, the proposed approach improves the content authentication rate and makes content validation simple and rapid. RSUs and caching vehicles collaborate to validate content signatures, reducing the probability of invalid data transmission. This ensures that only valid data would be transferred, stored, and obtained within VANET. The performance analysis of proposed and existing techniques is described in **Table 10**.

Table 10 clearly illustrates that the proposed technique provides efficient performance compared to other existing techniques such as ECCN, FCCN and IVC.

Table 10. Performance analysis.

Performance metrics	Technique used			
	ECCN	FCCN	IVC	Proposed
Verification accuracy (%)	91.7	93.96	96.47	**98.95**
Content authentication rate (%)	90.66	93.47	95.11	**97.83**
PDR (%)	89.31	92.77	95.93	**98.48**
FNR (%)	9.203	6.791	3.222	**1.064**
FPR (%)	8.117	5.486	2.992	**0.894**
Verification overhead (%)	8.786	5.882	4.012	**1.629**
End-to-End latency (s)	77.24	73.31	71.06	**67.24**

5.3 Verification Against Replay Attack and Fabricated Verification Reports

The proposed method uses a digital signature and a timestamp-based validation technique to ensure the integrity and authenticity of the transferred verification information. The originating node uses its cryptographic credentials to sign each verification report, which is transmitted between vehicles and RSU. Recipients can verify their identities using lightweight public-key infrastructure. The inclusion of timestamps and nonce values prevents replay attacks by ensuring that outdated or duplicated reports are rejected. Also, Bloom filters are used to quickly check the legitimacy of verification data while cross-verification among neighboring nodes enhances trustworthiness. This multi-layered approach enables vehicles and RSUs to confidently authenticate the source and integrity of verification information, which effectively mitigates the risks posed by malicious nodes attempting to inject fabricated or replayed reports.

5.3.1 Adaptive Probability Analysis for Probabilistic Verification

In the proposed protocol, the verification probability is adaptively set rather than fixed, allowing for a balance between security and efficiency. The probability dynamically adjusts based on network conditions, content popularity and assessed trust level of neighboring vehicles. The verification probability is increased to reduce the risk of unverified packet propagation for highly critical or frequently requested road safety data. The probability can be lowered to reduce the computational overhead for less critical or previously validated content. This adaptive mechanism also considers historical trust scores and feedback from verification exchanges to coverage conflicting verification states among vehicles, which ensures the system-wide consistency. The protocol reduces windows of vulnerability while preventing unnecessary resource consumption by using an adaptive context-aware approach, which preserves both trust and efficiency in highly dynamic vehicular environments.

5.3.2 Practical Deployment Feasibility

In this section, the feasibility of deploying the proposed dataset caching and delivery algorithm has been analyzed. While the algorithms are mathematically detailed, it was intentionally designed with lightweight operations such as RIVP-with a bloom filter and mobility-aware caching strategies to ensure compatibility with resource-constrained vehicular devices. The modular structure enables the simplification for real-world adaptation and reduces the computational and storage overhead. Future work involves extensive validation on real-vehicular testbeds to account for hardware limitations like memory, processing capacity and intermittent connectivity by ensuring the approach remains efficient, scalable and practical for deployment in a dynamic VANET environment.

5.4 Case Study Analysis by Addressing Real-world Security Failures in VANETs

Case 1: Data Spoofing in VANETs

Several reported incidents indicate that the adversaries broadcast falsified safety messages such as fabricated collision warnings or phantom traffic jams. It causes the vehicle to make unnecessary reroutes or emergency stops. The proposed RIVP with a bloom filter improves verification speed through probabilistic verification and cached validation. False positives inherent to bloom filters can occasionally allow the spoofed data through under high-load scenarios with large data volumes. Future work will integrate a digital signature with ML-based anomaly detection, which enables the routers to learn and flag unusual message pattern and cross-check content provenance. Thereby, it can reduce the chance of accepting the falsified data.

Case 2: Sybil Attacks in VANETs

Sybil attacks have been demonstrated where a single malicious vehicle generates multiple fake identities, overwhelming routing tables and undermining trust-based forwarding mechanism. Although the probabilistic verification of the proposed model can mitigate some of these attempts by requiring verification along multiple hops, RIVP alone does not fully eliminate the risk because attackers can create identities that appear valid within verification intervals. Future solution will integrate the identity validation frameworks, dynamic trust management and ML-based techniques that analyze spatio-temporal behavioral patterns to differentiate legitimate vehicles from Sybil nodes. It will strengthen the security and reliability of VANET communication.

5.5 Discussion

The proposed approach improves content validation efficiency by combining an RIVP with a Bloom filter which outperforms ECCN, FCCN, and standard IVC. The proposed approach reduces computing complexity and enhances processing speed compared to ECCN and FCCN by enabling stochastic verification through caching vehicles, which have significant verification overhead and delay authentication. The ECCN, FCCN, and IVC were selected due to their widely referenced advancements in VANET content validation which cover various aspects of efficiency, interest-based data delivery and fault tolerance. ECCN emphasizes energy-efficient content caching, FCCN focuses on fast and fault-tolerant content delivery and IVC addresses interest-based vehicular communication for dynamic dataset. These techniques provide a comprehensive baseline for evaluating the proposed model’s performance based on latency, secure data delivery and content verification accuracy. The proposed method reduces FPR and FNR, ensuring accurate authentication by selecting verified permanent packets and transmitting verification data. Also, unicast forwarding reduces network congestion by optimizing routing compared to ECCN's multi-hop technique. Compared to FCCN and standard IVC, the utilization of caching vehicles and RSUs achieves a higher PDR and a lower end-to-end delay by reducing redundant content retrievals. Compared to existing methods, this combination of effective validation, less verification overhead, and optimized transmission ensures better security, better content distribution along with improved vehicular network performance.

The proposed model achieves better performance by integrating mobility-aware dataset delivery with social attribute-based forwarding in order to reduce the content retrieval delays and delivery failures in VANET environments. It utilized request and response social attributes to identify the optimal forwarders, which ensures robustness against node mobility and broken paths. The RIVP with a bloom filter accelerates content authentication while maintaining high accuracy and reducing computational overhead. Also, efficient caching strategies reduce redundant transmissions and improve interest satisfaction rates. By integrating these techniques, it enhances throughput, lowers latency and improves reliability which makes the model more secure, adaptive and scalable compared to other existing techniques.

The proposed technique systematically resolves the limitations of existing VANET communication models through an efficient, adaptive and secure ICN framework. It reduces the content retrieval delay using IVC-based unicast forwarding and optimize the request/response social attributes that rapidly locate optimal caching members. Single-point failure issues are eliminated through RIVP with bloom filter-based authentication. Dynamic adaptability is achieved by using mobility-aware social-attribute weights that adjust to changing VANET topologies. Storage and verification were addressed with the compact Bloom filter, which enables fast hash-based validation and lightweight storage. Interest satisfaction rates improve through intermediate router interest aggregation and fair probabilistic verification and reduce delays. Prioritized forwarding reduces the complex packet latency, while caching verified datasets reduces redundant transmissions and sustains energy efficiency even in power-constrained vehicles. The comparative analysis of proposed model is represented in **Table 11**.

Table 11. Comparative analysis.

Author name and references	Year	Technique used	Performance
Bibi et al. (2024)	2024	A trust-aware VANET framework	-
Hlaing and Asaeda (2023)	2023	ISCM	Computational time – 80 ms
Lu et al. (2023)	2023	An anonymous protection mechanism	10 KB- communication overhead
Anisetti et al. (2022)	2022	A certification methodology for ICN	Average execution time 27 ms
Xue et al. (2022)	2022	SCD2 scheme	Response verification time – 2.694 ms
Al-Omaisi et al. (2024)	2024	GeoISA	67.8 % interest satisfaction rate (ISR) for 120 nodes
Qian et al. (2022)	2022	Forwarding strategy of interest packets	-
Gupta et al. (2023)	2022	An ICN-based energy-efficient placement of content	79 ms - content retrieval delay for 0.60 content popularity
Proposed	**2025**	**RIVP with bloom filter**	**98.95% - verification accuracy and 97.83 – content authentication rate**

5.5.1 Limitation

While the proposed model significantly improves data verification accuracy and reduces latency in VANETs through the utilization of RIVP with Bloom filter, several limitations remain. Initially, the evaluation of model is conducted in a controlled simulation environment, which may not fully represent the complexities of real-world VANET deployments, such as varying environmental condition, unpredictable vehicular mobility and so on. Although the caching and cooperative validation, especially in highly dynamic or adversarial scenarios. Also, the caching and cooperative verification mechanism may occur resource overhead such as memory and processing load on vehicles with limited computational capacity. These limitations will be considered for future work to further enhance the scalability, robustness and adaptability of proposed model.

5.6 Statistical Analysis

To further validate the robustness of proposed model, statistical significance tests are conducted to report the average performance metrics. The results were averaged over multiple independent runs and the mean, standard deviation (SD) and 95% confidence intervals (CI). Furthermore, a paired t-test was performed to analyze the performance of the proposed models. The p-values (less than 0.05) confirm that the observed improvements are statistically significant. This analysis illustrates that the proposed model's efficient performance is consistent and reproducible. The statistical test of proposed model is described in **Table 12**.

Table 12. Statistical analysis of proposed model.

Metric	Mean (%)	SD	95% CI	t-test (t value)	p-value
Accuracy	98.72	±0.41	[98.33 – 9.11]	6.27	0.002
Precision	98.35	±0.47	[97.91 - 98.79]	5.94	0.003
Recall	98.60	±0.38	[98.22 – 98.98]	6.11	0.002
F1-score	98.46	±0.36	[98.10 – 98.82]	6.42	0.001

5.7 Computational Overhead of Defense Mechanisms

While the proposed framework thoroughly addresses different attack scenarios in VANETs, it is equally important to consider the computational overhead incurred by each defence mechanism. Lightweight defenses such as probabilistic data verification and Bloom filter-based RIVP achieved minimal overhead, as they operate selectively and efficiently during high-traffic conditions. Conversely, more resource-intensive strategies like cryptographic signing, metadata validation and certificate management impose slightly higher computational costs, but these are justified by the significant gain in security and robustness against severe threats such as Sybil and replay attacks. Especially, the overhead is carefully balanced with the criticality of the attack scenario which ensures that lightweight defenses are applied to frequent, low-risk attacks, while stronger but more costly mechanisms are reserved for high-risk intrusions. It ensures that the proposed system enhances resilience against adversaries without compromising real-time efficiency, which makes it suitable for deployment in a safety-critical VANET environment.

6. Conclusion

This research developed an efficient and secure approach to ensure the validity and authentication of content in VANETs. In the proposed framework, vehicles on each road segment collaboratively generate datasets with various types of content. These datasets are transmitted using unicast forwarding, while caching vehicles store previously requested data to reduce the latency and improve response time. A probabilistic verification strategy is used, wherein vehicles validate the transient data packet with a certain probability and share verification results to improve the overall accuracy of the system. Each content provider signs the data and appends additional verification metadata by enabling intermediate nodes to authenticate the content efficiently. Also, edge nodes utilize the RIVP with bloom filter to rapidly verify content authenticity. The proposed model achieves 98.95% verification accuracy with an overhead of 1.629%. Despite its strengths, the proposed model still faces limitations in scalability and catching costs, especially in a highly dynamic vehicular environment. Future enhancements will focus on multi-cloud integration of improved scalability and robustness. For future work, two concrete directions are envisioned by conducting large-scale real-world deployment testing in urban and highway scenarios to validate scalability and robustness under dynamic vehicular condition. Extending the proposed framework by integrating it with emerging 5G/6G-enabled edge computing infrastructures to support ultra-low latency and high bandwidth vehicular applications. It will further enhance the practicality and adaptability of the proposed solution in next-generation intelligent transportation systems.

Conflicts of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

AI Disclosure

The author(s) declare that no assistance is taken from generative AI to write this article.

References

Ahmed, A.A., Kadhim, A.K., Najim, A.H., Alheeti, K.M.A., Satar, N.S.M., & Hashim, A.H.A. (2024). Improving VANET localization performance with data verification: challenges and solutions. In *2024 International Conference on Decision Aid Sciences and Applications* (pp. 1-6). IEEE. Manama, Bahrain. https://ieeexplore.ieee.org/document/10836346.

Ai, Z., Zhang, M., Zhang, W., Kang, J., Tong, L., & Duan, Y. (2023). Survey on the scheme evaluation, opportunities and challenges of software defined-information centric network. *IET Communications*, *17*(20), 2237-2274. https://doi.org/10.1049/cmu2.12694.

Ali, W., Din, I.U., Almogren, A., & Rodrigues, J.J. (2024). Federated learning-based privacy-aware location prediction model for internet of vehicular things. *IEEE Transactions on Vehicular Technology*, *74*(2), 1968-1978. https://ieeexplore.ieee.org/document/10462542.

Al-Omaisi, H., Sundararajan, E.A., Alsaqour, R., Abdullah, N.F., & Bakar, K.A.A. (2023). GeoISA: a new road-topology-assisted geo-based content discovery scheme for vehicular named data networking. *Vehicular Communications*, *40*, 100573. https://doi.org/10.1016/j.vehcom.2023.100573.

Alsayaydeh, J.A.J., Shkarupylo, V., Yusof, M.F.B., Oliinyk, A., Artemchuk, V., Ali, M.F., & Herawan, S.G. (2024). Dynamic network-based analytical model for information-centric networking implementation in 5G communication. https://doi.org/10.21203/rs.3.rs-4733809/v1.

Anisetti, M., Ardagna, C.A., Berto, F., & Damiani, E. (2022). A security certification scheme for information-centric networks. *IEEE Transactions on Network and Service Management*, *19*(3), 2397-2408. https://ieeexplore.ieee.org/document/9750109.

Bhardwaj, S., Harit, S., & Yadav, A. (2024). Towards a software-defined networking model for consumer-centric content delivery network for IoT. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4903. https://doi.org/10.1002/ett.4903.

Bibi, A., Jabbar, S., Saeed, Y., Iqbal, M.M., Ahmad, A., Akbar, H., & Qureshi, I. (2024). TR-Block: a trustable content delivery approach in VANET through blockchain. *IEEE Access*, *12*, 60863-60875. https://ieeexplore.ieee.org/abstract/document/10494579.

Chandra, A.T., Shivarudraiah, R.M., Gadde, N., & Nagarajappa, R.K.B. (2025). A novel scheme for enhanced content integrity, authentication, and privacy in information centric network using lightweight blockchain-based homomorphic integrity and authentication. *International Journal of Electrical and Computer Engineering*, *15*(1), 654-668. http://doi.org/10.11591/ijece.v15i1.pp654-668.

Gupta, D., Rani, S., Singh, A., & Rodrigues, J.J. (2023). ICN based efficient content caching scheme for vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, *24*(12), 15548-15556. https://doi.org/10.1109/TITS.2022.3171662.

Hlaing, H.H., & Asaeda, H. (2023). Ensuring content integrity and confidentiality in information-centric secure networks. In *2023 IEEE 20th Consumer Communications & Networking Conference* (pp. 810-816). IEEE. Las Vegas, USA. https://ieeexplore.ieee.org/document/10060672.

Hou, J., Tao, T., Lu, H., & Nayak, A. (2023). An optimized gnn-based caching scheme for sdn-based information-centric networks. In *GLOBECOM 2023 IEEE Global Communications Conference* (pp. 401-406). IEEE. Kuala Lumpur, Malaysia. https://ieeexplore.ieee.org/document/10437541.

Jiang, S., Li, J., Sang, G., Wu, H., & Zhou, Y. (2024). Vehicular edge computing meets cache: An access control scheme with fair incentives for privacy-aware content delivery. *IEEE Transactions on Intelligent Transportation Systems*, *25*(8), 8404-8418. https://ieeexplore.ieee.org/document/10423916.

Lim, H. (2024). Toward infotainment services in vehicular named data networking: a comprehensive framework design and its realization. *IEEE Transactions on Intelligent Transportation Systems*, *26*(2), 2793-2810. https://ieeexplore.ieee.org/document/10752355.

Lu, Y., Wang, C., Yue, M., & Wu, Z. (2023). Consumer-source authentication with conditional anonymity in information-centric networking. *Information Sciences*, *624*, 378-394. https://doi.org/10.1016/j.ins.2022.12.051.

Mahaveerakannan, R., Tamilvizhi, T., Rayen, S.J., Khalaf, O.I., & Hamam, H. (2024). Information centric networking based cooperative caching framework for 5G communication systems. *Computers, Materials & Continua*, *80*(3), 1-22. https://doi.org/10.32604/cmc.2024.051611.

Mazhar, S., Rakib, A., Pan, L., Jiang, F., Anwar, A., Doss, R., & Bryans, J. (2024). State-of-the-art authentication and verification schemes in vanets: a survey. *Vehicular Communications*, *49*, 100804. https://doi.org/10.1016/j.vehcom.2024.100804.

Pruthvi, C.N., Yashitha, K., Rekha, R., HS, V., & Shreyas, J. (2023). Information-centric caching solutions for vehicular networks: a survey. In *2023 4th International Conference on Computation, Automation and Knowledge Management* (pp. 1-6). IEEE. Dubai, United Arab Emirates. https://ieeexplore.ieee.org/document/10449511.

Qaiser, F., Al Harthy, K.S., Hussain, M., Frnda, J., Amin, R., Gantassi, R., & Zakaria, M.D. (2025). Classifications and analysis of caching strategies in information-centric networking for modern communication systems. *Engineering Reports*, *7*(2), e70005. https://doi.org/10.1002/eng2.70005.

Qian, J., Yu, Y., & Chang, X. (2022). A delay-based interest packet forwarding strategy in vehicular named data networking. In *2022 2nd Asia-Pacific Conference on Communications Technology and Computer Science* (pp. 351-356). IEEE. Shenyang, China. https://doi.org/10.1109/ACCTCS53867.2022.00078.

Rizwan, S., Husnain, G., Aadil, F., Ali, F., & Lim, S. (2023). Mobile edge-based information-centric network for emergency messages dissemination in internet of vehicles: a deep learning approach. *IEEE Access*, *11*, 62574-62590. https://ieeexplore.ieee.org/document/10158680.

Sajini, S., Anita, E.M., & Janet, J. (2023). A block chain based authentication scheme in VANET for a secure data communication using SHAH algorithm. *Indian Journal of Science and Technology*, *16*(46), 4291-4299. https://doi.org/ 10.17485/IJST/v16i46.2010.

Sangi, A.R., Anamalamudi, S., Alkatheiri, M.S., Enduri, M.K., Carie, A., & Alqarni, M.A. (2023). Redundant transmission control algorithm for information-centric vehicular IoT networks. *Computers, Materials & Continua*, *76*(2), 2217. https://doi.org/10.32604/cmc.2023.038305.

Sharma, D., Elmagzoub, M.A., Alghamdi, A., Alrizq, M., Yadav, K., Sharma, S., & Prashanth, V. (2024). Entity-aware data management on mobile devices: utilizing edge computing and centric information networking in the context of 5G and IoT. *Mobile Networks and Applications*, *29*(2), 448-459. https://doi.org/10.1007/s11036-023-02224-5.

Singh, A., Rani, P., Ramesh, J.V.N., Athawale, S.V., Alkhayyat, A.H., Aledaily, A.N., & Sharma, R. (2024). Blockchain-based lightweight authentication protocol for next-generation trustworthy internet of vehicles communication. *IEEE Transactions on Consumer Electronics*, *70*(2), 4898-4907. https://ieeexplore.ieee.org/document/10400828.

Tan, X., Wang, S., Ji, L., Tong, X., Zou, C., Zheng, Q., & Yang, J. (2023). Hybrid-coding based content access control for information-centric networking. *IEEE Transactions on Wireless Communications*, *23*(7), 6765-6777. https://ieeexplore.ieee.org/document/10327691.

Wang, F., & Hou, R. (2024). V2R/V2V collaborative interest forwarding method for vehicular named data networking. In *2024 IEEE/CIC International Conference on Communications in China* (pp. 197-202). IEEE. Hangzhou, China. https://doi.org/10.1109/ICCC62479.2024.10681999.

Wang, X., & You, X. (2024). Efficient data sharing and caching for information-centric IoT. *IEEE Internet of Things Journal*, *11*(10), 18074-18081. https://ieeexplore.ieee.org/document/10416892.

Xue, K., He, P., Yang, J., Xia, Q., & Wei, D.S. (2022). SCD2: Secure content delivery and deduplication with multiple content providers in information centric networking. *IEEE/ACM Transactions on Networking*, *30*(4), 1849-1864. https://ieeexplore.ieee.org/document/9732194.

Yang, B., Guo, Y., & Chen, X. (2023a). Privacy-oriented coded caching in mobile information-centric networking. In *2023 Asia Pacific Signal and Information Processing Association Annual Summit and Conference* (pp. 1556-1563). IEEE. Taipei, Taiwan. https://ieeexplore.ieee.org/document/10317189.

Yang, J., Chen, L., Tang, J., Li, J., & Yang, W. (2023b). Swarm reinforcement learning for collaborative content caching in information centric networks. In *ICC 2023-IEEE International Conference on Communications* (pp. 384-390). IEEE. Rome, Italy. https://ieeexplore.ieee.org/document/10278917.

Zhang, J., Jiang, Y., Cui, J., He, D., Bolodurina, I., & Zhong, H. (2022). DBCPA: dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks. *IEEE Transactions on Mobile Computing*, *23*(2), 1127-1141. https://ieeexplore.ieee.org/document/9994052.

Publisher's Note- Ram Arti Publishers remains neutral regarding jurisdictional claims in published maps and institutional affiliations.