# SYSTEMATIC REVIEW OF VEHICULAR AD-HOC NETWORKS TRUST-BASED MODELS

Samson W. Nyutu, John G. Ndia and Peter M. Mwangi

Murang'a University of Technology,School of Computing and Information Technology,
Murang'a, Kenya

## ABSTRACT

*Vehicular Ad-hoc Networks (VANETs) are specialized type of Mobile Ad-hoc Networks (MANETs) developed to support vehicle-to-vehicle and vehicle-to-infrastructure communication. Security threats in these networks include malicious nodes, Man-in-the-Middle (MitM) attacks and Denial of Service (DoS) attacks which threaten network reliability. Trust-based models in VANETS seek to evaluate trust of nodes and data sharedand incorporate certain features which enhance adaptivity. This systematic literature review (SLR) analyses the adaptive trust-based models available in VANETs with an emphasis on the features that facilitate adaptability in the dynamic environment. The review follows Barbara Kitchenham (2007) systemic approach and accesses databases including Google Scholar, IEEE Xplore and Wiley Online Library where 34 articles are included. The findings highlight important characteristics such as historic data analysis, real-time behavior monitoring, adaptive trust score update, frequency of messages, context awareness and real-time detection of intrusive attacks that make the VANETs trust models more adaptable.*

## KEYWORDS

*Vehicular Ad-hoc Networks (VANETs), Mobile Ad-hoc Networks (MANETs), adaptiveness, dynamic network, Man-in-the-Middle (MitM) attack, Internet of Things (IoT)*

## 1. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) are a subset of Mobile Ad-hoc Networks (MANETs) and are in particular enabled to facilitate communication between vehicles and between vehicles and roadside units (RSUs) in a smart city [1] . VANETsinterface with wireless network technology and vehicles are equipped with sensor devices to make them communicate effectively by use of Internet of Things (IoT) technology [1].

VANETs are aimed at managing traffic, providing safety and make better experience to the driver and passengers in the transport sector [2] .Connected vehicles and road-side units in these networks are termed as nodes and they share important information (e.g. traffic controls, prevention of road accidents and warnings) and do this in two separate communication methods, Vehicle-to-Vehicle (V2V) as well as Vehicle-to-Infrastructure (V2I) communication [2].

Due to their ad hoc nature, VANETsare highly susceptible to internal and external security attacks [3] . According to [3] , the manner in which VANETs operate including open wireless medium, speedy vehicles and trust dependency expose the networks to security attacks including man-in-the-middle attack, sybil attack, denial of service and messages tampering.

DOI:10.5121/ijwmn.2025.17406

Trust amongst nodes is a very important aspect to consider in a reliable, safe and efficient operation of VANETs [1] [2] . In this context, researchers are triggered to develop trust-based models in VANETs due to the demanding need of secure, reliable and efficient communication environment. The figure below illustrates an adaptive trust protocol in VANET[3].

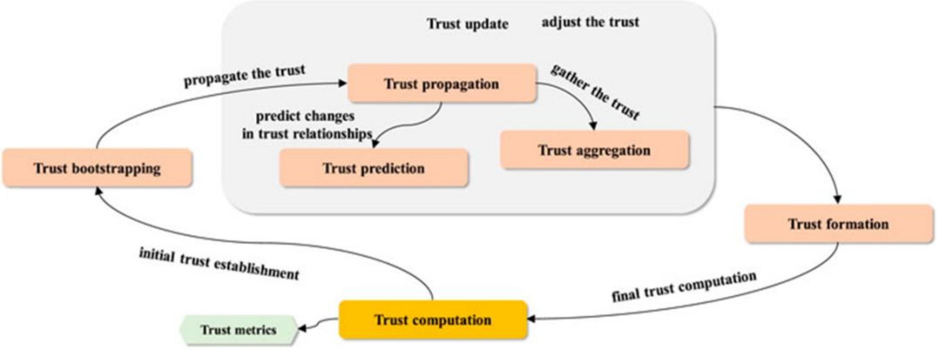

Figure 1.An architecture of Adaptive VANET Trust Model

## 2. Related Work

In recent years, several systematic literature reviews (SLRs) have been conducted to evaluate trust management in VANETs. However, they consistently fall short of addressing the need for adaptiveness of trust-based models in a highly dynamic vehicular environment.

Tyagi et al. (2020) focused exclusively on trust and reputation mechanisms in VANETs, analyzing over 90 peer-reviewed studies [4]. In their work, trust models have been categorized into direct trust, indirect (recommendation-based), hybrid and reputation-driven frameworks. However, there is over-reliance on static trust scores which make it difficult to apply the approach in flexible and scalable networks.

In another review, Che et al. (2022) presented a comprehensive review of trust management models in VANETs, including emerging domains such as blockchain integration, machine learning-based trust evaluation and software-defined networking (SDN)[5]. However, the review also note that context-aware and behavior-adaptive trust models are still underdeveloped.

A more recent review by El-Deeb et al. (2023) emphasize on trust management within Internet of Vehicles (IoV) domain, incorporating cloud computing and fog-based architectures [6] . The study identified scarcity of adaptive models capable of instant context switching or behavior-triggered trust adjustment.

This systematic literature review is positioned to address adaptability of trust models in VANETs.

## 3. Research Method

This research was carried out as a systematic literature review based on Barbara Kitchenham's original guidelines (2007) to systematically review existing trust-based models in VANETs.

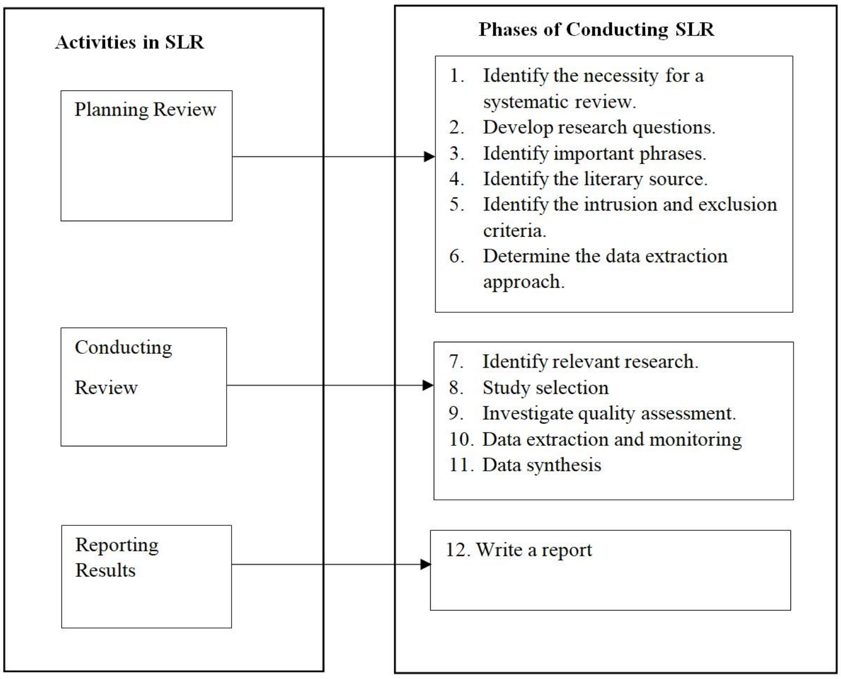
Activities in SLR
Planning Review
Conducting Review
Reporting Results
Phases of Conducting SLR
1. Identify the necessity for a systematic review.
2. Develop research questions.
3. Identify important phrases.
4. Identify the literary source.
5. Identify the intrusion and exclusion criteria.
6. Determine the data extraction approach.
7. Identify relevant research.
8. Study selection
9. Investigate quality assessment.
10. Data extraction and monitoring
11. Data synthesis
12. Write a report

Figure 2.SLR Process

## 3.1. Research Questions

The key purpose of this systematic literature review is to formulate and define questions which covers concrete analysis of trust-based models in Vehicular Ad-hoc Networks including their features. In this research work, two research questions were formulated and they were answered based upon our collated studies.

The research questions used are: -

i. What are the existing trust-based models in Vehicular Ad-hoc Networks (VANETs)?
ii. Which features make adaptive trust-based models in VANETs?

## 3.2. Search Strategy

To ensure a comprehensive and systematic review of trust-based models in Vehicular Ad-hoc Networks (VANETs), the researcher employed a well-defined search strategy. Search strategy was composed of four steps including defining keywords, forming search string, selection of sources and search process.

### 3.2.1. Defining Keywords

Keywords were defined for each question to the most relevant results of the paper. For this study, the research revolves around trust-based models in VANETs with an emphasis of the adaptive features in those models. Formulated questions were also searched using these keywords in order to retrieve the most relevant data about our topic. The list of all various keywords used are as shown in the table below.

Table 1. Research Questions with Keywords

| Research Questions | Keywords |
|---|---|
| What are the existing trust-based models in Vehicular Ad-hoc Networks (VANETs)? | “Trust-based Models AND VANETs” OR “Vehicular Ad-hoc Networks AND Trust” |
| Which features make adaptive trust-based models in VANETs? | “Adaptive Trust-based Models AND VANETs”<br>“Trust evaluation OR trust-based models AND VANETs" |

### 3.2.2. Forming Search String

A search string was formed based on the keywords for each research question [7] . The process involved deriving major terms from the topic and research questions, identifying spelling or synonyms for major terms, identifying keywords, using Boolean operator OR for synonyms or alternating spellings and linking of major terms with Boolean AND operator.

As a result of the above defined steps, the following search string was created.

(“Adaptive trust-based models” OR “dynamic trust evaluation”) AND (“VANETs” OR “Vehicular Ad-hoc Networks”).

### 3.2.3. Selection of Sources

Several academic databases and search engines including Google Scholar, IEEE Xplore Digital Library and Wiley Online Library were used. These platforms were selected due to their vast range of scholar resources relating to security and trust in Ad hoc networks[8].

Table 2. Online data sources

| Database Source | Link or Website |
|---|---|
| Google Scholar | https://scholar.google.com |
| IEEE Xplore Digital Library | https://ieeexplore.ieee.org/Xplore |
| Wiley Online Library | https://onlinelibrary.wiley.com |

### 3.2.4. Search Process

In order to find the relevant primary studies, the researcher focused on literature published in the last five years in the academic databases listed in Table 2 above. The above-mentioned search string was run on all databases in the Table 2 and retrieved 2,750 search results in Google Scholar, IEEE Xplore Digital Library returned 932 search results and Wiley Online Library produced 1,045 search results.

The discrepancies in the amount and character of search results were noted, where Google Scholar returned more results than that in other sources because it indexes a wider array of materials. IEEE Xplore and Wiley, on the contrary, made an emphasis on peer-reviewed content. To eliminate these inconsistencies using Kitchenham SLR guideline, the researcher employed stringent screening and quality search, to eliminate irrelevant and insignificant studies.

### 3.2.5. Documenting Search Strategy

Our search strategy documentation was inspired by [9] . In this review, the search strategy was carefully documented to provide a clear account of how relevant studies were identified and selected. Key components of the documented search strategy included, databases and search engines as listed in the Table 2 above, Search Strings illustrated in the forming search string section, time frame of literature published in the last five years and included and excluded studies listed in the Table 3 below.

Table 3. Included and Excluded Studies details

| **Database Source** | **Included** | **Excluded** | **Total** |
|---|---|---|---|
| Google Scholar | 16 | 46 | 62 |
| IEEE Xplore Digital Library | 7 | 22 | 29 |
| Wiley Online Library | 11 | 77 | 88 |
| **Total** | **34** | **145** | **179** |

The documentation guided in the assessment of search and helped to keep track of search. A detailed documentation of search has been depicted in the Table 4 shown below.

Table 4. Document of Search Strategy

| **Database Source** | **No. of papers retrieved with the keywords** | **No. of papers with filter (by years)** | **No. of papers excluded** |
|---|---|---|---|
| Google Scholar | 323 | 62 | 261 |
| IEEE Xplore Digital Library | 212 | 29 | 183 |
| Wiley Online Library | 416 | 88 | 328 |

### 3.2.6. Inclusion and Exclusion Criteria

The researcher established criteria for including and excluding studies as follows:

**Inclusion Criteria:**

a) Peer-reviewed journal articles, conference papers and book chapters.
b) Studies focusing on adaptive trust-based models in VANETs.
c) Papers discussing features like dynamic trust adjustment, node behavior, communication patterns or historical data.

**Exclusion Criteria:**

a) Non-peer-reviewed articles or non-English publications.
b) Papers not focusing on adaptive trust models or unrelated to VANETs.
c) Outdated studies (published more than five years ago).

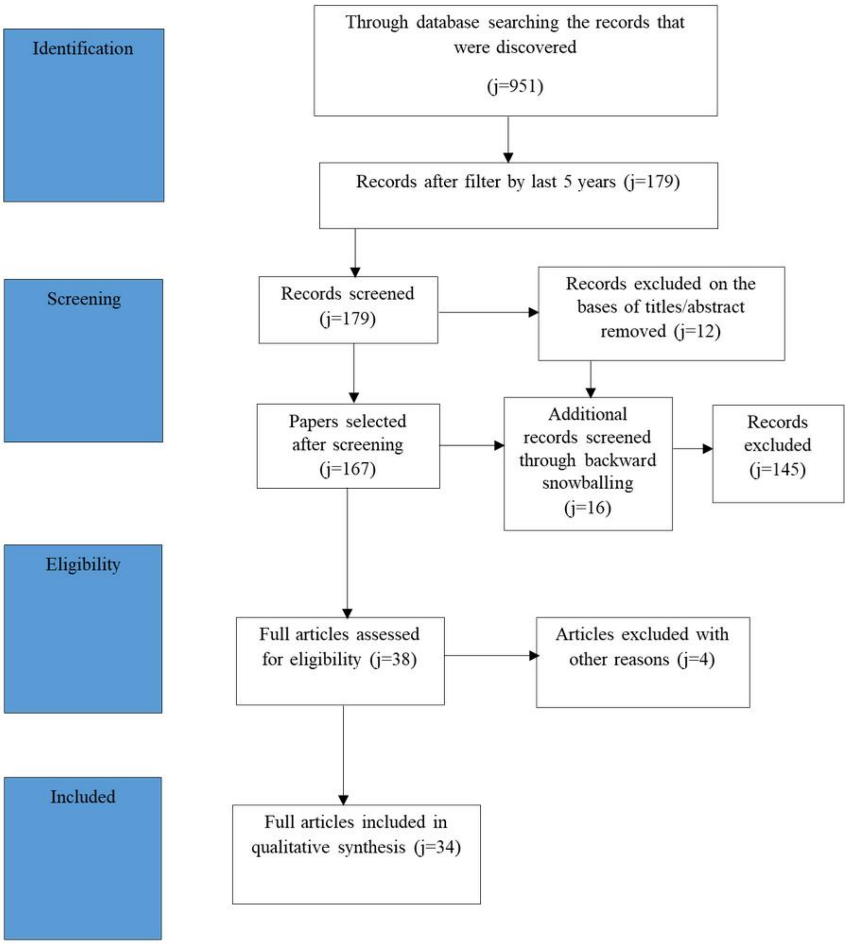
Identification
Through database searching the records that were discovered (j=951)
Records after filter by last 5 years (j=179)
Screening
Records screened (j=179)
Records excluded on the bases of titles/abstract removed (j=12)
Papers selected after screening (j=167)
Additional records screened through backward snowballing (j=16)
Records excluded (j=145)
Eligibility
Full articles assessed for eligibility (j=38)
Articles excluded with other reasons (j=4)
Included
Full articles included in qualitative synthesis (j=34)

Figure 3.Flowchart for selection of articles

### 3.2.7. Quality Assessment

Quality assessment criteria were used to evaluate the reliability, validity and relevance of selected studies in systematic reviews and was based upon [10] . A checklist for the quality assessment questions (QAs) was created, against which each research paper was checked in order to select the more relevant studies that would furnish desired answers to the research questions.

Table 5.Quality Assessment Questions

| Q.ID | Quality Assessment Questions |
|---|---|
| QA1 | Does the study address features specific to adaptive trust-based models in VANETs? |
| QA2 | Are key features like dynamic trust adjustment, historical data integration addressed? |
| QA3 | Is the methodology for analyzing trust models well documented? |
| QA4 | Does the study use performance metrics (e.g precision, recall, F-Score) |
| QA5 | Does the study include real-world testing or validation of the adaptive trust model? |
| QA6 | Does the study make significant contribution to advancing trust-based models in VANETs? |

A Quality Assessment checklist consisting of six questions was applied to examine the articles using a score of Yes (1), Partial (0.5)and No (0) to indicate the responses. The scores were added up to obtain an Aggregate Value (A.V). Those papers that had A.V 2.5 or more were accepted otherwise rejected. Among all works reviewed, 34 papers were above the threshold, whereas 145 were excluded. Across all the 34 studies, an average Aggregate Value (A.V) was 4.8/6.0, where all papers scored greater than 3.5.

## 4. Overview Of Selected Studies

This section discusses the research questions answered in details to meet the objectives of the research questions identified for the study.

### 4.1.Rq1. What are the Existing Trust-Based Models in Vehicular Ad-Hoc Networks (Vanets)?

Vehicular Ad-Hoc Networks (VANETs) are crucial for enabling communication among vehicles and roadside infrastructure, ensuring secure and efficient traffic management [11] [12] . The dynamic nature of VANETs makes them vulnerable to security threats which aim to compromise nodes and data shared over these networks [13] . To address these challenges, researchers have developed various trust-based models aimed at ensuring secure and reliable communication by evaluating the trustworthiness of participating nodes.

Ahmad et al. proposed a concept of hybrid trust model called MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles [2] designed to mitigate the common MitM attacks in Vehicular Ad-hoc Networks (VANETs). In VANETs, security and trust are required to ensure reliable and secure communication [5] . MARINE combines both data and node centric computations to assess the trust of both the nodes and data [2] . It however makes use of fixed trust levels and is not flexible to the changing environment unlike adaptive models which updates their trust scores in real-time [2].

Singh et al. (2021) took the approach of resolving the scalability and consistency of trust issues as experienced in traditional trust management frameworks based on blockchain [14] . The architecture implicates smart vehicles, RSUs and Regional Authorities, where vehicles report their suspicion of behavior through a smart contract. Trust chains are kept dynamically updated where good vehicles earns and bad vehicles lose. However, the model presumes that vehicles can identify misbehavior without any help and can be limited by blockchain such as delay and collusion [14].

Siddiqui et al. researched a new context-aware trust model to support the Internet of Vehicles (IoV) systems, given flexibility and avert attacked-based [15] . Computation of trust relies on direct observations and indirect recommendations. RSUs compute global trust via elements of weighting by frequency. The model becomes versatile, using dynamic misbehavior thresholds and time-based forgetting to enhance effective response to selective and on-off attacks. It however makes the assumption that data is perfectly monitored in lossy networks and has high computational overhead as the trust score has to be regularly updated [15].

According to Sarker et al. (2023), they proposed a reinforcement learning-based neighbor selection scheme and adaptive trust management that can be used in secure VANET routing [16]. Trust is calculated using a hybrid and an integration, comprising of Bayesian belief (direct trust) and Yager rule (indirect trust). Q- learning chooses the forwarding node with the trust scores updating the Q -tables. The adaptive characteristics entail a learning rate obtained as a result of mobility, time-decayed trustand a fusion of trust based on confidence. The model is resistant to on-off attacks and also to the changes in topology, though it is computationally costly and needs accurate GPS or speed data [16].

To increase the security and reliability of the VANETs, Gupta and Sagar (2024) put forward a decentralized trust-based model [17] .Trust is calculated through direct interactions and indirect recommendations. The model also guarantees safe communication using a cryptography approach such as key generation, digital signatures and public key encrypting. It is learning on the basis of how it changes the trust scores on the basis of frequency and real-time behavior. High computational requirements in the dense networks and the assumption of stable communication are some of the issues to be encountered with the model in enhancing the resilience of VANET [17].

The research by Cheong et al. (2024) suggested the Path-Backtracking-Based Trust Management Scheme (PBTMS) in VANETs to identify malicious nodes [18]. The model puts both entity trust based past communication together with path trust-based message route. RSUs employ path-backtracking and find the points of message corruption to update the trust levels. The real-time behavior analysis, adaptive thresholds and time decay are adaptive features. Although it can be used to isolate malicious nodes, the model is not scalable to high-density VANETs because of the paths and multi-metrics that are computationally demanding [18].

Recently, Zhao et al. (2025) proposed DMTAS-VB, a trust assessment strategy relying on Dynamic Model Update of VANETs blockchain-based DMTAS [19] . The model applies real time behavior analysis and federated learning to update the trust classifications and does not expose the raw data, maintaining privacy. Blockchain brings about the immutability of trust scores and the integrity of decisions. DMTAS-VB takes an evolving approach to identify such attacks as Sybil and false data injection. Nonetheless, its intensive overhead on training of models and blockchain consensus makes it less scalable and applicable in dense VANETs with limited computation capabilities [19].

The table below presents a comparative overview of the existing VANET trust-based models, as discussed in the RQ1.

Table 6. Analysis of Existing VANET Trust-based Models

| **Trust Model** | **Adaptive Features** | **Strengths** | **Weaknesses** |
|---|---|---|---|
| MARINE Trust Model[2] | Does not incorporate adaptive features | Hybrid trust evaluation, simple and lightweight | Relies on static and predefined trust scores. |
| Blockchain-Based Adaptive Trust Management in IoV[14] | Updates trust scores lively, real-time vehicle behavior detection andcontext awareness | Resistant to tamperingand offers transparency and traceability. | High workloads and computational expenses. |
| Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the IoV[15] | Context awareness past interactions of vehicles and real-time behavior analysis | High-quality protection against attacks increasing network reliability | Difficulty in modeling different contextual parameter and high computational cost. |
| Reinforcement Learning Based Neighbor Selection for VANET with Adaptive Trust Management[16] | Realtime learning for attack detection and recommendations from neighbors | Minimizes the effects of malicious nodes and supports network scalability. | Needs extensive training time and complex data computation. |

| | | | |
|---|---|---|---|
| A Trust-Based Framework for Enhancing Security and Reliability in VANETs [17] | Vehicle behavior, Message frequency, recommendation from neighbors, adjust trust scores on real-time | Make networks more secure and reliable by detecting and isolating malicious nodes. | Increased communication overheads given frequent alterations of trust. |
| A Path-Backtracking-based Trust Management Scheme for VANETs[18] | Historical data integration,dynamictrust score adjustment. | Increases the accuracy of trust paths and recognition of malicious nodes by backtracking. | Complexity in computations caused by path tracking and scalability problems. |
| DMTAS-VB: [20] | Dynamic trust score update, recent vehicles interaction and behavior patterns. | Builds accuracy of trust continuously by updating the model. | Greater computational complexity brought by blockchain incorporation. |

## 4.2. Which Features Make Vanets Trust-Based Models Adaptive

Adaptive trust-based models in Vehicular Ad-hoc Networks (VANETs) are designed to dynamically respond to changes in network conditions, node behaviors and malicious attacks [21] [22] . This research questions answers the key features that enable trust models in VANETs to be adaptive.

### 4.1.1. Analysis from the Literature

Historical data integrationis a key feature that enhances the adaptivity of trust-based models in Vehicular Ad-hoc Networks (VANETs). These models have better evaluations as they are capable of evaluating trust based not only on current behavior in real-time, but are also based on cumulative behavioral patterns by including records of past interactions. As an example, the works of DMTAS-VB: Dynamic Model Update-Based Trust Assessment Strategy for VANETs Considering Blockchain [19] use current and previous data in flexibly updating trust values. Interaction history is recorded and stored permanently and securely in blockchain as a deterministically irreversible store, assuring that the data cannot be compromised. Because the model uses this historical overview, the model can keep adjusting the judgment of trust as time progresses, to be more accurate in identifying unreliable or harmful vehicles.

The model Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles [15] proposes a context-aware model and considers some contextual elements including historic values of trust in history and environmental factors like location, type of vehicle, and time. It measures the vehicle behavior on repeated interactions at different contexts and has the ability to perform adaptive trust-scoring, which evaluates repeated interactions independently of behavioral consistency as influenced by contextual factors. This will avoid sudden alterations of trust and introduce fairness to trust computation.

In A Path-Backtracking-based Trust Management Scheme for VANETs [18], the model relies on the past data that walks through communication paths and assess the conduct of the intermediate nodes in these paths. Previous interactions are analyzed by the system by doing a backtracking and identifying patterns of cooperative misbehavior or selective forwarding, which may be missed by stateless models. All-in-all the incorporation of past information enables trust-based VANET models to change in response to ever-changing requirements, identify the long-term threats, personalize trust related actions and increase general network security and reliability.

Real-time behavior analysisis the most crucial adaptive functionality of trust-based models in VANETs. It allows quick evaluation of the vehicle actions and timely reaction to the possible threat. In the Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract [14], messages are processed in real time to update trust values and smart contracts are used to process behavioral inputs on an automated basis comprising of message consistency, mobility patterns and data integrity. Blockchain will make such updates irreproachable and smart contacts will introduce rules that will immediately change the level of trust when new evidence of behavior is generated.

Likewise, Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles [15] employs real-time data in continuous monitoring of automobile transmissions and fusing it with the contextual factors, current location, the condition of the road and the traffic density. This enables the model to instantly identify the misrepresentation of normal behavior of a child and adjust the level of trust accordingly protecting any misbehavior in time.

As indicated in A Trust-Based Framework for Enhancing Security and Reliability in Vehicular Ad-hoc Networks [17] , real-timer behavior monitoring is a heartbeat of determining trustworthiness. Direct encounters are measured with the framework and the behavior of the communication is being studied, such as packet forwarding, delaying messages and answering styles. Trust scores are instantaneously adjusted to the current reliability of the vehicle and this makes the network more responsive to attacks that include blackhole attack or Sybil attack.

Finally, DMTAS-VB [20] uses rapidly updated models together with real-time analysis of interactions. The system also gathers the evidence about the behavior based on recently generated interactions and makes it instantly relevant to the historical data and adjusts the score of trust on-the-fly. This combination of present and previous conduct permits a strong and flexible process of trust appraisal. All together these models prove that trust management in VANETs requires real time behavior analysis.

Dynamic trust score adjustmentis another key feature to enhance adaptivity of trust-based models in VANETs, enabling systems to respond changing behavior of vehicles and network conditions. In the Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract model [14], smart contracts posted on a block chain actively update the trust scores. Such smart contracts assess real-time and past behavior analytics, including message consistency, location and mobility rates and set corresponding trust ratings without human intervention. Trust data jumps in the blockchain technology that provides integrity, transparency, and immutability of the data and makes possible decentralized and automated modifications in trust information without central control.

Here, in the Path-Backtracking-based Trust Management Scheme for VANETs [18], trust score adjustment is based on the scrutiny of path and the actions of the nodes in those paths. Upon detecting suspicious or uncommon conduct, the model identifies the path of transmission of the message in reverse to come up with nodes that cannot be trusted. Adaptations are in place wherein the trust scores are readjusted when there is a discovery of forwarding behavior or packet drops or variations when there has been backtracking. This is a method of making adaptive trust decisions with consideration of the short-term behavior along with a consideration of the context of a communication path.

Finally, DMTAS-VB model [19] improves progressive adaptation adding a history of the vehicle related to its past interactions and behavior pattern. The modelinvolves incorporating all benefits of historical data securely stored on a blockchainand update the trust rating every time a vehicle is encountered. Its trust evaluation plan is dynamic, adjusting the scores continuously according to how vehicles exhibit trustworthy or malicious behavior. Together with current evidence, this historical context allows DMTAS-VB to have a flexible and precise trust evaluation system that is particularly appropriate in very flexible VANET scenarios.

Context awarenessenhances adaptivity in robust VANETs environments by adjusting trust evaluations basedon the environmental conditions.This feature allows models to make trust decisions based on vehicles behavior patterns, congestion in the network and situations relevant to each interaction. For instance, in Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles [15] ,the model combines environmental and situational variables such as location of the vehicle, vehicle speed, time of the day, traffic congestion and type of the road with respect to the trust evaluation module. Continuous evaluation of behavior along with these parameters allows the system to differentiate malicious activity and legitimate behavior in a given situation. Activities such as a regular braking on a highway can be suspicious but on city road it is a normal situation. Such a strategy increases the accuracy of trust and reduces false positives to a considerable extent.

In the work of [14] , context awareness is incorporated in the logic of smart contracts in the blockchain technology. Although decentralized and secure control of trust management provided by the blockchain is the essential thing referred to in this model, in the case of smart contracts, one may introduce the so-called contextual inputs such as the vehicle location, relevance of the message and the mobility patterns. Such context-dependent conditions assist in the live modification of trust scores according to the condition during the generation of data or observation of behavior. It is not quite as context-specific as “Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles” model [15] , but this model allows a flexible platform to support context-driven rules. Both models allow showing that the context awareness is crucial to adjusting trust estimation to the actual road conditions and enhancing the robustness of VANET trust systems.

Real-time learning for attack detectionhas also been identified as a key feature for adaptive trust modelsin VANETs. According to “Reinforcement Learning Based Neighbor Selection for VANET with Adaptive Trust Management” [16] , the model introduces real-time learning capabilities to enhance attack detection in vehicular networks. With the help of reinforcement learning (RL), the trust scores and the policies of neighbor selection are updated through a continuous observation of node behavior. Vehicles are regarded as the agents who are trained about the best decision-making procedures through experimentation in regard to a reward function by punishing malicious action and rewarding cooperation. It is a real-time learning and therefore nodes with abnormal behavior of ignoring messages, corrupting or even just selective transmission of messages are quickly detected and isolated.

Unlike other models, this model has the advantage of refining itself through time by adapting to consistent interaction with the network environment. The RL based approach constantly upgrades its policy as it accumulates additional evidence of behaviorthus increases its precision in the identification attacks schemes unlike in the case of static trust models. This renders it very applicable in large and decentralized VANET environment, where the attackers could switch their strategies very quickly. The model besides enhancing the detection of malicious nodes it enhances the overall reliability and safety of networks by making intelligent trust-informed routing choices through real-time trust estimation and learning.

Message frequencytoo plays an important role in adaptive trust models inVehicular Ad Hoc Networks (VANETs) as it is used to assess node reliability and detect potential attacks such as flooding, Sybil or message suppression. To check how confidently and correctly vehicles communicate in the network, a message frequency is monitored in [17] . In this model, abnormalities like unusual high rate of messages can be an indication of flooding attacks, whereas irregular communication may indicate selective forwarding or misbehavior. These observations are factored into the frameworks multi-metric estimation of trust and trust scores are mutable to adjust to the consistency of communications. This aids in isolating malicious nodes in a short period and that routing of the messages will be done using trusted members.

On the same note, DMTAS-VB: Dynamic Model Update-Based Trust Assessment Strategy for VANETs [19] , involves frequencies of different messages in the application of real-time evaluation of trust. Vehicle interaction is continuously monitored followed by the study of rate and reliability of messages over time. Regular and consistent messages are usually a sign of more trustworthiness and irregular or communication that is too frequent are a red flag. DMTAS-VB, by means of combining message frequencies with other predictors and historical trust records keeps scores of trusts responsive and accurate. These rapid frequency usages of messages help the model to always stay ahead of the emerging threat and maintain stability of trust on highly volatile and decentralized basis of VANETs.

### 4.1.2. Expert Analysis

To validate the findings of the systematic literature review on adaptive trust-based models in VANETs, data was collected through expert-based questionnaires targeting specialists in the domain. A total of 31 responses were received.Purposive sampling was used to obtain the opinion of experts with credible and relevant feedback experience on VANETs.To ensure reliability of the responses, a baseline evaluation of the respondents' level of knowledge on the VANETs was done.Based on their rankings, 2 were rated as having extremely low knowledge and 3 as low, and thus were excluded. The remaining 26 responses, representing individuals with moderate to high knowledge, were analyzed using descriptive statistics in IBM SPSS Statistics version 26.0.

The frequency distributions were calculated in order to determine the expert perception of the several adaptive features of trust-based models such as the integration of historical data, behavioral analysis in real-time, dynamic tracking of adjustments to the trust score, context awareness, attack detection through real-time learning and the tracking of message frequency. In addition, thematic analysis of open-ended responses revealed three common features including privacy preservation, live behavior monitoring and scalability. Among these, live behavior monitoring aligned directly with literature, while scalability was associated with context awareness. However, privacy preservation, though important, was not identified in the literature as an enabler of adaptivity in trust models of VANETs.

## 5. DISCUSSION

This paper presents the systematic literature review (SLR) of trust-based mechanisms in the Vehicular Ad-hoc Networks (VANETs) with the approach (Kitchenham, 2007). Thirty-four peer-reviewed works with publications between 2019 and 2025 were chosen according to the pre-designed inclusion and exclusion criteria. The analysis showed that there are some existing trust-based models in VANETs that are hybrid in nature meaning they use both data-centric and node-based calculations and are adaptive in dynamic vehicular network environments.

The review discoveredimportant features which while integrated in a model of VANET, they make the model adaptive. Among the noted key features, one can distinguish the use of historical data, real-time monitoring of vehicles behavior, automatic adjustment of the trust score, message frequency detection, real-time learning for attack detection and context-based assessments. Adaptive trust models in VANETs will not only be more accurate and timelier to detect malicious behavior, but can further adapt to instant updates and location-specific context, making them more resilient than static models. They can however be more demanding on computational resources and optimization can be important to allow practical deployment.

## 6. Conclusion

The findings of this review confirm that adaptive features such as using historical data, real-time behavior processing, dynamic trust score update and monitoring message frequency increases the capacity of VANET trust models to identify malicious nodes and ensure a secure network. These features can be introduced to protocols such as the lightweight, hybrid MARINE protocol to enhance responsiveness, reliability and resistance against man-in-the-middle attacks.

Future work shouldcombineadaptive mechanisms and context awareness and real-time learning to develop secure, scalableand adaptable trust systems to handle different vehicular conditions. This would facilitate continuous learning, quicker responses to threatsand effective work under various traffic conditions and would contribute to the creation of interoperable security standards in intelligent transportation systems.

## References

[1] Xia, Hui, Z. shun, L. Ye, Zhen, P. kuan and P. Xin, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 7108-7120, 2019.

[2] Ahmad, Farhan, K. Fatih, A. Asma, H. Rasheed and H. Fatima, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3310-3322, 2020.

[3] Rashid, Kanwal, S. Yousaf, A. Abid, J. Faisal, A. Reem and M. Ammar, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," Sensors, vol. 23, no. 5, p. 2594, 2023.

[4] A. K. Tyagi, K. Mohan, M. Shaveta and M. N. Meghna, "Trust and reputation mechanisms in vehicular ad-hoc networks: A systematic review," Advances in Science, Technology and Engineering Systems Journal , vol. 5, no. 1, pp. 387-402, 2020.

[5] Che, Haoyang, D. Yucong, L. Chen and Y. Lei, "On trust management in vehicular ad hoc networks: A comprehensive review," Frontiers in the Internet of Things , vol. 1, p. 995233., 2022.

[6] Rehman, Abdul, H. Mohd and Y. Kwang, "State-of-the-art IoV trust management a meta-synthesis systematic literature review (SLR)," PeerJ Computer Science, vol. 6, no. 1, p. 334, 2020.

[7] Mendes and Emilia, "Search strategy to update systematic literature reviews in software engineering," 2019.

[8] Muzammal, S. M., M. Raja and J. Noor, "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186-4210, 2020.

[9] Lefebvre, Carol and G. Julie, "Searching for and selecting studies," Cochrane Handbook for systematic reviews of interventions, pp. 67-107, 2019.

[10] Paul, Justin and Harshleen, "Frameworks for developing impactful systematic literature reviews and theory building: What, why and how?," Journal of Decision Systems, vol. 33, no. 4, pp. 537-550, 2024.

[11] Hussein and Rasheed, "Trust in VANET: A survey of current solutions and future research opportunities," IEEE transactions on intelligent transportation systems, vol. 22, no. 5, pp. 2553-2571, 2020.

[12] Sateesh and Hritik, "State-of-the-art VANET trust models: Challenges and recommendations," 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020.

[13] Tripathi, N. Kuldeep and S. Subhash, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," International Journal of System Assurance Engineering and Management, vol. 11, no. 2, pp. 426-440, 2020.

[14] Singh, K. Pranav, N. Sunit, G. Kayhan, R. Danda and N. Sukumar, "Blockchain-based adaptive trust management in internet of vehicles using smart contract.," IEEE Transactions on Intelligent Transportation Systems , vol. 22, no. 6, pp. 3616-3630, 2021.

[15] Siddiqui, A. Sarah, M. Adnan, Z. S. Quan, S. Hajime and N. Wei, "Trust in vehicles: toward context-aware trust and attack resistance for the internet of vehicles," IEEE Transactions on Intelligent Transportation Systems , vol. 24, no. 9, pp. 9546-9560, 2023.

[16] Sarker, Orvila, S. Hong and B. M. Ali, "Reinforcement learning based neighbour selection for VANET with adaptive trust management," IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 85-594, 2023.

[17] G. a. Sagar, "A Trust-Based Framework for Enhancing Security and Reliability in Vehicular Ad-hoc Networks (VANETs)," International Conference on Computing, Sciences and Communications (ICCSC), pp. 1-6, 2024.

[18] Cheong, Chaklam, S. Yujie, C. Yue, L. Chee and W. Xinyuan, "A Path-Backtracking-Based Trust Management Scheme for VANETs," IEEE 99th Vehicular Technology Conference (VTC2024-Spring), pp. 1-6, 2024.

[19] Y. Li, X. Yawen, L. Qi and L. Jiangtao, "DMTAS-VB: Dynamic Model Update-based Trust Assessment Strategy for VANETs Considering Blockchain," 2025.

[20] Li, Yufeng, X. Yawen, L. Qi and L. Jiangtao, "DMTAS-VB: Dynamic Model Update-based Trust Assessment Strategy for VANETs Considering Blockchain," IEEE Internet of Things Journal (2025), 2025.

[21] Zhang, Song, L. Yanbing, X. Yunpeng and H. Rui, "A trust based adaptive privacy preserving authentication scheme for VANETs," Vehicular Communications, vol. 37, 2022.

[22] Aslan and Sen, "A dynamic trust management model for vehicular ad hoc networks," Vehicular Communications, vol. 41, p. 100608, 2023.

## AUTHORS

**Samson Waweru Nyutu**, is an experienced Information Technology professional and a Cisco Certified Network Associate (CCNA). He earned a Bachelor of Science degree in Information Technology from Dedan Kimathi University of Technology in 2018 and is currently pursuing a Master’s degree in Information Technology at Murang’a University of Technology, Kenya. His research interests include Computer Networks, Cybersecurity and Data Mining. He is a professional member of the Computer Society of Kenya.

**John Gichuki Ndia**, is a Senior Lecturer in the Department of Information Technology and he is currently the Dean School of Computing and Information Technology, Murang'a University of Technology, Kenya. He earned his Bachelor of Information Technology from Busoga University in 2009, and his MSc. in Data Communications from KCA-University in 2013. He pursued his PhD in Information Technology at Masinde Muliro University of Science and Technology in 2020. His research interests include Software quality, artificial intelligence applications in software engineering, computer network protocols, and computer networks security. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM)

**Dr. Peter Maina Mwangi**, is a Lecturer at the Department of Computing and Information Technology, Mama Ngina University College, Kenya. He received his BSc. in Computer Science from Busoga University, Uganda in 2010, his MSc in Data Communication and Networks from KCA University, Kenya in 2018 and his PhD in Computer Science from Murang’a University of Technology, Kenya in 2024. His research interest is in Computer Networks, Security, Artificial Intelligence. He is a Professional Member of the Institute of Electrical and Electronics Engineers (IEEE), the International Association of Engineers (IAENG) and the Scientific & Technical Research Association (STRA)