Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.072281

ARTICLE

A Novel Signature-Based Secure Intrusion Detection for Smart Transportation Systems

Hanaa Nafea[1], Awais Qasim[2], Sana Abdul Sattar[2], Adeel Munawar[3], Muhammad Nadeem Ali[4] and Byung-Seo Kim[4,*]

[1]College of Computer Science and Engineering, Taibah University, Al-Madinah Al-Munawwarah, 42353, Saudi Arabia
[2]Department of Computer Science, GC University Lahore, Lahore, 54000, Pakistan
[3]Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani, 12121, Thailand
[4]Department of Software and Communication Engineering, Hongik University, Sejong-City, 30016, Republic of Korea

*Corresponding Author: Byung-Seo Kim. Email: jsnbs@hongik.ac.kr

Received: 23 August 2025; Accepted: 29 October 2025; Published: 12 January 2026

ABSTRACT: The increased connectivity and reliance on digital technologies have exposed smart transportation systems to various cyber threats, making intrusion detection a critical aspect of ensuring their secure operation. Traditional intrusion detection systems have limitations in terms of centralized architecture, lack of transparency, and vulnerability to single points of failure. This is where the integration of blockchain technology with signature-based intrusion detection can provide a robust and decentralized solution for securing smart transportation systems. This study tackles the issue of database manipulation attacks in smart transportation networks by proposing a signature-based intrusion detection system. The introduced signature facilitates accurate detection and systematic classification of attacks, enabling categorization according to their severity levels within the transportation infrastructure. Through comparative analysis, the research demonstrates that the blockchain-based IDS outperforms traditional approaches in terms of security, resilience, and data integrity.

KEYWORDS: Smart transportation; intrusion detection; network security; blockchain; smart contract

1 Introduction

The rapid advancement of smart transportation systems has brought about significant improvements in efficiency, safety, and convenience. Traditional Intrusion Detection Systems (IDS) have limitations in terms of centralized architecture, lack of transparency, and vulnerability to single points of failure [1]. Signature-based intrusion detection depends on a database of known attack patterns or signatures to identify and prevent malicious activities [2]. By enhancing the immutable and distributed nature of blockchain, this approach can be enhanced with improved data integrity, transparency, and resilience against tampering or manipulation. The decentralized architecture of blockchain eliminates single point of failure, ensuring the continuous availability and reliability of the IDS [3]. Smart transportation systems encompass a wide range of technologies and applications focusing on enhancing the efficiency, safety, and sustainability of transportation systems. Intelligent traffic management systems, autonomous cars, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, and intelligent transportation management centers are just a few of the components that these systems combine. The communication and data sharing of

these components allow the monitoring, decision making, and optimization of real-time transportation operations [4].

1.1 Attacks on Smart Transportation Systems

Smart transportation systems are more susceptible to cyberattacks as a result of their growing reliance on digital technologies and network connectivity. Attacks are defined as unwelcome access by an individual or group aiming to harm, plunder, or misuse confidential and sensitive information belonging to an individual or organization. Potential attacks may include everything from malware infections and unauthorized access to data breaches and distributed denial-of-service (DDoS) attacks, as well as physical disruptions caused by compromised systems. Serious repercussions of these risks can include jeopardized security, interrupted operations, monetary losses, and infrastructure damage [5]. Table 1 lists some of the most common types of attacks on smart transportation systems.

Table 1: Common attack types on smart transportation systems

Attack name	Definition of the attack	Mode of prevention
Man-in-the-middle (MITM) attack	The attacker intercepts and manipulates communication between two parties in order to steal, alter, or inject information.	Implement strong encryption algorithms and secure communication protocols.
Data injection attack	The attacker inserts malicious data or code into the system to alter records, disrupt processes, or expose sensitive information.	Employ intrusion detection systems (IDS) and validate input data.
Spoofing attack	The attacker impersonates a legitimate node within the network to gain unauthorized access, manipulate data, or steal information.	Use robust authentication mechanisms and update cryptographic keys frequently.
Denial-of-service (DoS) attack	The attacker overwhelms the system or server with excessive traffic, exhausting resources, and preventing legitimate communication.	Conduct traffic analysis, apply rate limiting, and use anomaly detection systems.

1.2 Traditional Intrusion Detection Systems

In many different fields, traditional IDS have been used extensively to identify and stop cyber-attacks [6]. Usually, these systems use anomaly-based or signature-based detection techniques. While anomaly-based IDS looks for departures from typical system behavior, signature-based IDS employs a database of known attack patterns or signatures to find and stop malicious activity. Furthermore, it can be difficult to update and maintain the signature database, particularly in light of the constantly changing nature of cyber threats [7,8]. The swift progress of intelligent transportation systems, distinguished by the incorporation of Internet of Things gadgets, connected vehicles, and intelligent infrastructure, has significantly enhanced the efficiency and safety of urban mobility. However, in case of attacks, IDS becomes inefficient as it does not have access to the valid conditions of the attacks.

Blockchain is a distributed ledger system that operates decentralized manner, allowing record-keeping to be transparent and safe without requiring a central authority. Because blockchain can improve trust,

security, and traceability, it has drawn a lot of attention from a variety of industries, including finance, supply chain management, and healthcare [9]. Blockchain technology and signature-based intrusion detection can be combined to create a transparent and decentralized smart transportation network security system. A signature-based IDS system is essential for a smart transportation system using blockchain because it provides an additional layer of security to detect and respond to known attack patterns and signatures. By detecting and responding to known attack patterns and signatures, a signature-based IDS system can help prevent financial loss, reputation damage, and disruptions to the transportation system [10]. This research focuses on solving the problem of database manipulation by an attacker by using a signature-based intrusion detection system tailored for smart transportation networks, incorporating blockchain technology to maximize the security, reliability, and transparency of the detection process.

The rest of this paper is organized as follows. In Section 2, we discuss the limitations of the related work and how the proposed approach overcomes these limitations. Section 3 provides a comprehensive explanation of the proposed framework. In Section 4, we demonstrate the application of the proposed framework using a case study. Section 5 concludes the paper.

2 Related Work

In [11], a novel approach for intrusion detection in IoT networks is discussed. The system works to detect intrusions in real-time, learn from other nodes in the network, and improve detection accuracy while reducing false positives. But the collaborative IDS model, while scalable, assumes homogeneous device behavior and static network topologies, which do not reflect the dynamic and heterogeneous landscape of smart transportation environments. In [12], the authors present a novel approach to enhance the accuracy of IDS using blockchain technology. The working of the approach involves integrating a blockchain-based framework with traditional IDS, where blockchain is utilized to store and organize intrusion detection rules, and to ensure the integrity and immutability of the detection data. Their limitation is that the proposed model operates in a generic computing/networking environment, not accounting for the real-time, mobile, and safety-critical nature of smart transportation systems. The authors of [13] have proposed a distributed intrusion detection system (DIDS), which detects and reacts to cyber-attacks instantly by utilizing cloud computing and blockchain technologies. Their approach relies heavily on cloud computing, which introduces significant latency and centralized dependencies, unsuitable for high-speed vehicular networks that require local, edge-level intrusion detection and response.

In [14], the purpose of the Blockchain-Enabled Intrusion Detection System (BIDS) is to improve security and efficiency in identifying and addressing cyber threats in smart cities. Their approach lacks a threat model tailored to vehicular networks and emphasizes collaborative intelligence across static nodes, which may not work efficiently in a highly dynamic, mobile transportation environment. In [15], federated learning and blockchain technology are used in the proposed Federated Intrusion Detection System (FIDS) for blockchain-based smart transportation systems to improve efficiency and security. But their approach relies heavily on computationally intensive ML models that increases overhead on resource-constrained vehicular devices. This, in turn, introduces delays in detection and response, which are unacceptable in high-speed transportation environments. The potential of using blockchain for intrusion detection in an intelligent transportation system is highlighted in [16]. However, they discussed the IDS integration conceptually but didn't present a specific detection technique (e.g., signature-based, anomaly-based), nor do they detail the detection logic or threat model.

According to [17], the distribution of cyber-attack signatures is a critical component of IDS. CIoTA (Collaborative IoT Anomaly Detection via Blockchain) is a decentralized framework that leverages blockchain technology to enable collaborative IoT anomaly detection. Their model is designed for static or low-mobility

IoT devices, and does not address the challenges of highly mobile nodes (e.g., vehicles in VANETs). The authors of [18] proposed a technique that builds a decentralized network of edge nodes and Internet of Things devices that exchange threat intelligence and anomaly detection models via a blockchain. But their approach focuses on blockchain-specific behaviors and anomalies, such as unexpected transactions, blocks, or peer behavior, rather than network-level or communication-layer attacks relevant to smart transportation systems. The application of blockchain technology to collaborative intrusion detection based on trust is investigated in [19], and they suggest an architecture that makes use of the tamper-proof nature of blockchain technology. But the approach lacks consideration of latency, mobility, and real-time communication challenges faced in vehicular environments. A distributed intrusion detection system is necessary for next-generation networks, such as 5G and the Internet of Things, because of their size, complexity, and dynamic nature. This plan uses machine learning, artificial intelligence, and advanced analytics to construct a network of agents that monitor and analyze traffic locally [20]. However, their model is for infrastructure-centric network environments and is not suited for vehicular or transportation systems, where nodes are highly mobile. The authors in [21–23] recommend the use of blockchain for improved security in IoTs. In Table 2, we provide a comparison table of our related work.

Table 2: Comparison table of the related work

Related Work	Method/Technique	Limitation
[18]	Collaborative blockchain-based signature IDS for IoT	Their approach is limited to IoT devices, lacks efficiency for large-scale transportation systems and the consensus overhead is not optimized.
[19]	Consensus algorithm for collaborative signature IDS	Their focus is on the consensus mechanism only. The approach has high latency under large network load and lacks integration with real transport systems.
[20]	Blockchain-based IDS accuracy enhancement	Their approach, although it improves detection accuracy, but does not address database manipulation or attack classification.
[21]	Distributed IDS using Blockchain + Cloud	Their approach is dependent on cloud that creates potential latency and privacy issues. Hence, the approach is not lightweight enough for real-time smart transport.
[22]	BIDS: blockchain-enabled IDS for smart cities	The proposed work is focused on Smart cities and does not explicitly address signature-based severity classification.
[23]	Federated IDS in blockchain-based smart transportation	They handled distributed detection of attacks, limited attack categorization, but the proposed method has high computational overhead due to federated learning.

The comparative analysis of existing intrusion detection approaches reveals several common limitations that hinder their effectiveness in securing smart transportation systems. Traditional IDS solutions such as blockchain-based models [12,13,15], and [16] often suffer from high consensus overhead and latency issues when deployed in large-scale environments. Several works [14,16–18], and [20] fail to provide fine-grained intrusion categorization or severity-based classification, limiting their applicability for real-time threat prioritization. Moreover, critical aspects such as database manipulation remain largely unaddressed in studies like [14,15,18], and [19], leaving systems exposed to tampering attacks. Additionally, many proposed

models [12,16,20] are tailored to generic IoT or smart city contexts, rather than transportation-specific infrastructures. These gaps collectively highlight the need for a novel framework that ensures decentralized security, mitigates database manipulation, and incorporates signature-based severity classification specifically for smart transportation systems.

3 Proposed Blockchain-Based Intrusion Detection for Smart Transportation Framework

Our proposed framework, Blockchain based Intrusion Detection for Smart Transportation (BIDST), is shown in Fig. 1. There are two major modules: Blockchain Initialization and Intrusion Detection Module. Below we will explain the working of each module in detail.

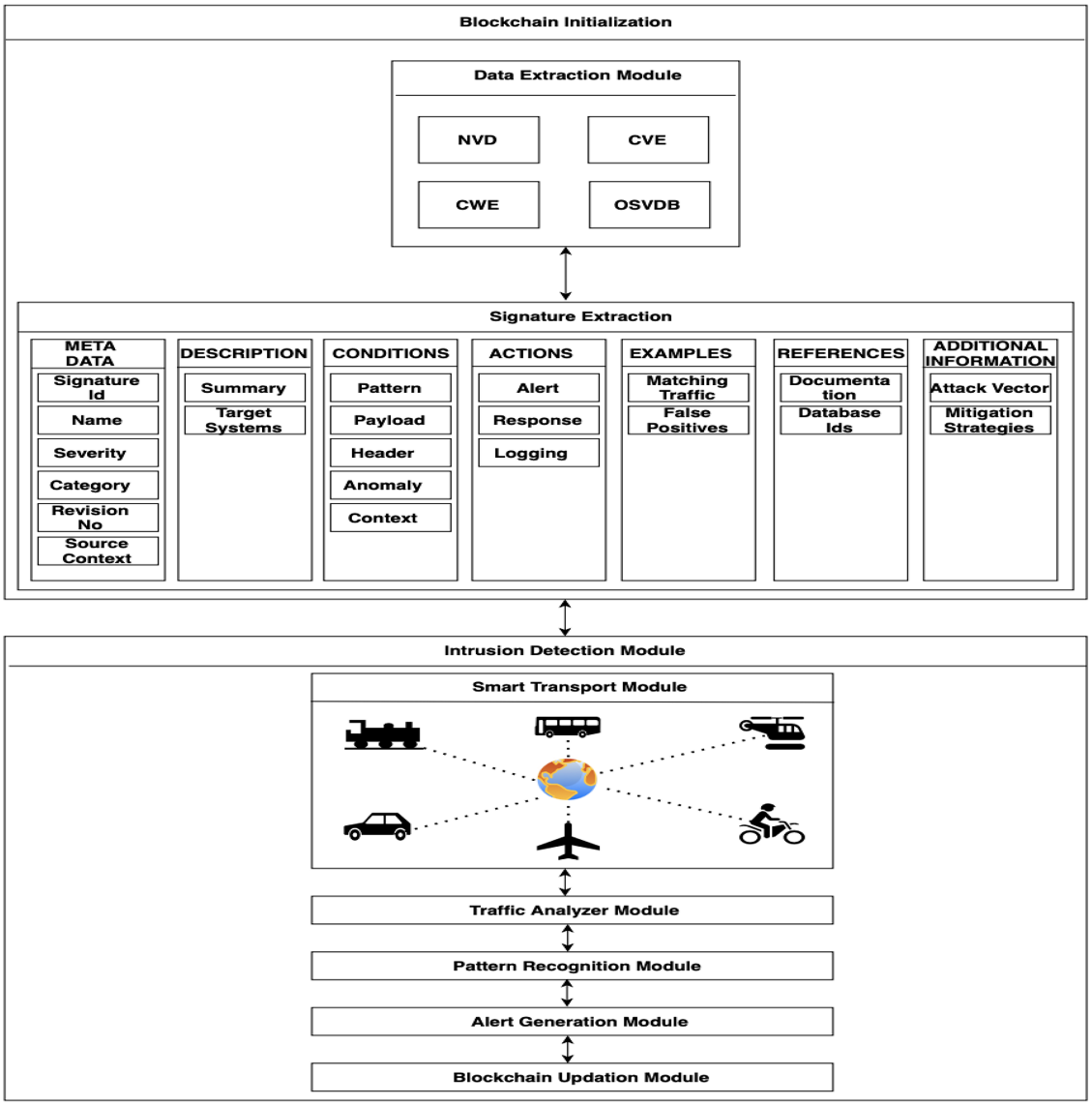

Figure 1: Proposed blockchain-based intrusion detection for smart transportation framework

3.1 Blockchain Initialization

This module is responsible for making sure that before the system is deployed it has signatures of all the common attacks on smart transportation systems. It has two submodules, i.e., Data Extraction Module and Signatures Extraction.

3.1.1 Data Extraction Module

This module will extract the data of common attacks from four repositories. The designer of the system can provide help in this to narrow down which attacks are most common. The whole purpose of keeping data of attacks in blockchain is to make it secure from attacks. In such attacks the attacker can manipulate the signatures of the attack rather than attacking on system's data. This can have severe consequences, like the intrusion detection failing because of compromised signatures. For our framework we have selected four repositories.

National Vulnerability Database (NVD): This database is managed by the National Institute of Standards and Technology (NIST). We can use it to identify vulnerabilities in software and hardware components of transportation systems, such as traffic management software, vehicle control systems, and communication protocols.

Common Vulnerabilities and Exposures (CVE): This database contains a list of publicly disclosed information security vulnerabilities and exposures. We can use it to match network traffic against known vulnerability patterns, helping to identify and prevent attacks on transportation networks.

Common Weakness Enumeration (CWE): It is a database of a community-developed list of common software security weaknesses. It helps to identify the root causes of vulnerabilities, making it easier to prevent and detect them.

Open-Source Vulnerability Database (OSVDB): It is an open-source vulnerability database that provides comprehensive information about vulnerabilities.

3.1.2 Signatures Extraction

This is the major contribution of our framework where we have designed the signature for our intrusion detection system. The signature is generic enough to capture all the details of common attacks on smart transportation systems. The signature defines the characteristics of the threat, the conditions under which the signature will trigger an alert, and the actions to be taken. The details of the attributes are given below.

3.2 Attributes of BIDST Signatures

The signature has seven sections as listed in Table 3. The section Meta Data contains information about the metadata of an attack. The section Description provides a summary of an attack. The section Conditions provides information about patterns/rules that can be used to detect an attack. The section Action contains information about what actions should be taken in case an attack is detected. The section Examples provides some sample traffic of the attack. The section References is useful if we want to get more information about an attack. It can contain links to the official documentation. Lastly, the section Additional Information contains information about how the attack is commonly carried out.

Table 3: Attributes of signatures to be used in the proposed BIDST framework

Tag	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
Meta data	Signature ID: unique identifier for the signature.	Name: descriptive name indicating the type of attack detected.	Severity: threat level (low, medium, high, critical).	Category: attack type (e.g., DoS, malware, unauthorized access).	Revision number: version of the signature for updates and tracking.	Source context: storage of contextual information.
Description	Summary: brief description of the detected behavior or threat.	Target systems: systems, devices, or networks applicable (e.g., web servers, IoT).	NA	NA	NA	NA
Conditions	Pattern/Rule: specific rules that define malicious activity.	Payload content: strings, commands, or patterns in the payload.	Header information: attributes like IP, ports, and protocols.	Anomalous behavior: deviations from normal behavior (e.g., unusual traffic).	Timing: repeated requests within a short interval.	Contextual information: additional conditions such as presence of files, services, or user actions.
Actions	Alert: type of alert generated (e.g., log entry, SOC notification).	Response: automated actions (e.g., block traffic, terminate session).	Logging: details recorded for analysis.	NA	NA	NA
Examples	Matching traffic: example packet or log triggering the signature.	False positives: possible sources of false positives and mitigation.	NA	NA	NA	NA
References	Documentation: links or references to technical resources.	CVE IDs: known vulnerabilities if applicable.	NA	NA	NA	
Additional information	Attack vector: method typically used (e.g., phishing, network-based).	Mitigation strategies: recommended preventive measures.	NA	NA	NA	NA

3.3 Smart Contract for Saving Signatures in Blockchain

In this section, we write a smart contract to store the signatures of common attacks in blockchain. The complete code is provided in the supplementary file. The smart contract is written in Solidity Language and it is implemented on the Ethereum blockchain. When the system is deployed then if a new attack is recognized then it will also be saved in it. The smart contract includes structures to store various details, including the signature ID, metadata, description, conditions, actions, examples, references, and additional information. We have created seven structs namely Metadata, Description, Conditions, Actions, Examples, References, Additional Information to store the signatures data. We can call the storeSignature function with the required data to store an IDS signature. The function emits an event, SignatureStored, to log the addition of a new signature. The getAllSignatures function allows retrieving all stored signatures.

3.4 Intrusion Detection Module

This module is responsible for monitoring all the traffic being communicated in a smart transportation system. It monitors not only the outbound traffic but also the traffic exchanged locally between the nodes of the system. This is to ensure that in case a compromised node tries to initiate an attack from within the system, it can be easily traced.

Smart Transportation System: This module represents the working of an STS, which will integrate advanced technologies and data analytics to enhance the efficiency, safety, and sustainability of transportation networks. It will comprise smart vehicles like smart cars, smart trains, smart planes, communication networks, data processing, and automation to manage and improve transportation in real-time. The major purpose of this system will be to improve traffic flow, enhance safety, increase cost efficiency, and provide user convenience.

Traffic Analyzer Module: In this module, the collected data will be processed to optimize traffic flow by adjusting traffic signals, providing real-time route guidance, and managing congestion.

Pattern Recognition Module: The purpose of this module is to detect patterns of data that will lead to any intrusions.

Alert Generation Module: This module will only be used if the system detects an intrusion. The designer of the system can decide what type of alerts he wants to be raised and what type of mitigation strategies need to be adopted.

Blockchain Updation Module: In case a new attack is detected that does not match with any of the previously stored signatures then its signatures will be saved in the blockchain for future.

The complete working of the proposed BIDST framework is presented in Algorithm 1.

Algorithm 1: Signature-based intrusion detection using blockchain

1: **Input:** Network Traffic Data, Signature Database [NVD, CVE, CWE, OS-VDB]
2: **Output:** Detect Intrusion, Generate Alert, Save New Signature in Blockchain
3: **procedure** StoreSignature(Metadata, Description, Conditions, Actions, Examples, References, AdditionalInfo)
4: CreateNewSignatureObject()
5: StoreSignatureOnBlockchain()
6: EmitEventLog()
7: **end procedure**
8: **procedure** GenerateReport(LoggedData, DetectionMetrics)
9: AnalyzeData()
10: IncludeStatistics(attack types, sources, frequency, response effectiveness)
11: ShareReportWithStakeholders()
12: **end procedure**
13: **START**
14: Initialize IDS components (Blockchain Signature DB, Detection Engine, Alert System)
15: CaptureNetworkTraffic()
16: **for** each packet in captured traffic **do**
17: ExtractRelevantFeatures()
18: CompareFeaturesWithDatabase()
19: **if** match found **then**
20: IntrusionDetected()
21: TriggerAlert(); LogDetails(); ExecutePredefinedResponse()
22: GenerateReport()
23: **else if** suspicious activity **then**
24: CreateNewSignatureObject(); StoreSignature(); EmitEventLog()

(Continued)

Algorithm 1 (continued)

```
25:             GenerateReport()
26:         else
27:             NoIntrusionDetected()
28:         end if
29: end for
30: END
```

Algorithm 1 demonstrates how the proposed BIDST framework begins by initializing the core components of the Intrusion Detection System (IDS), including the blockchain-based signature database, detection engine, and alerting system. Network traffic is continuously captured and processed, with relevant features extracted from each packet. These features are then compared against the existing signature database. If a direct match is found, the system immediately detects an intrusion, triggers alerts, logs the details, and executes predefined responses while generating a comprehensive report. In cases where the traffic does not match any known signature but exhibits suspicious activity, the system dynamically creates a new signature, stores it securely on the blockchain to ensure immutability and transparency, and emits an event log for auditability. Reports are also generated to summarize attack types, sources, frequencies, and response effectiveness. If neither a match nor suspicious activity is identified, the traffic is classified as benign, and the system continues monitoring.

4 Application of the Proposed BIDST Framework

In this section, we will show the working of the proposed BIDST framework with the help of a case study. Fig. 2 shows the working of a smart transportation system. In this system, various cars interact seamlessly to create a more efficient, safe, and user-friendly transportation environment. The connected vehicle will receive real-time traffic updates from the Regional Processing Unit (RPU), allowing it to reroute to avoid congestion. At the same time, the vehicle communicates with nearby traffic lights to ensure that it hits green lights along the way, further reducing travel time. Every vehicle needs to be preregistered in the system for it to be part of the blockchain. The RPU will use real-time data from sensors, cameras, and connected vehicles to monitor and manage traffic flow. It will help in optimizing traffic signal timings, managing congestion, and reducing travel times. To improve traffic flow and reduce congestion, the RPU will modify the timing of traffic signals based on current traffic circumstances. The RPU is initialized with signatures of common attacks on smart transportation systems, and every message before being sent to a vehicle is scanned for suspicious activity.

4.1 Intrusion Attempt on a Car

The intrusion detection system will scan the incoming network packets that are being sent to cars. These packets can be from other cars or from outside the private blockchain territory. The RPU will compare the data against our database of known attack signatures. In case a match is found, the RPU will trigger the alert. Otherwise, if there is certain network traffic activity that is not present in our database, but it is categorized as malicious then the IDS will ask for human intervention before saving the signature of the suspicious activity.

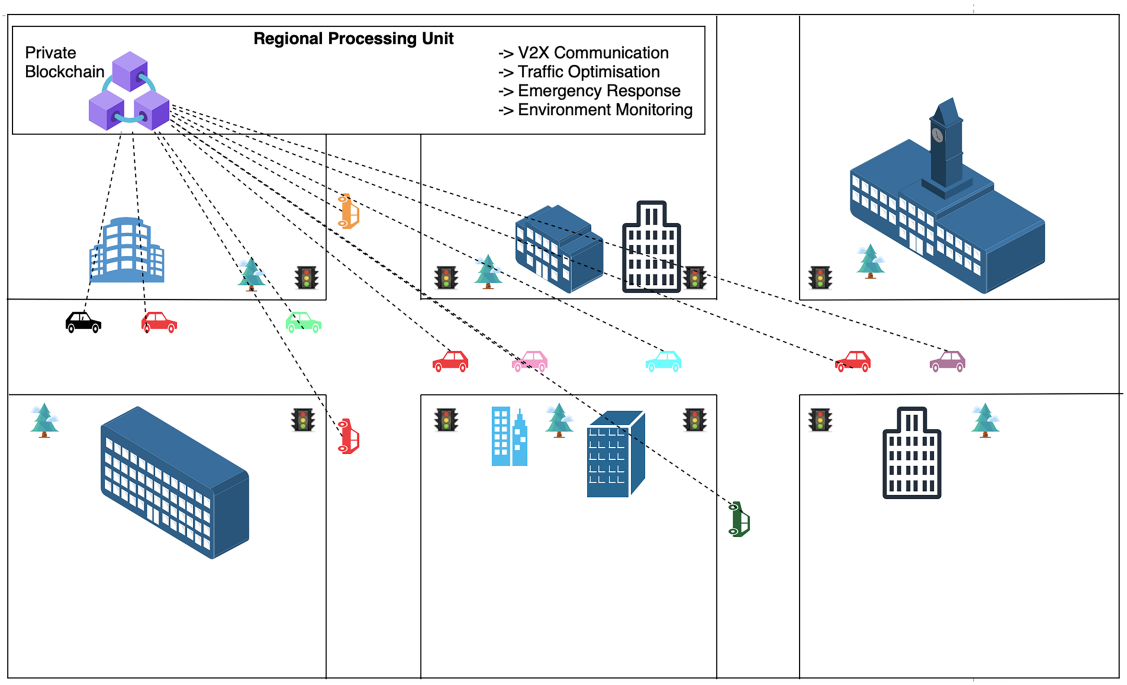

Figure 2: A sample smart transportation example

Sample Network Traffic with SQL Injection Attempt

Fig. 3 is an example of network traffic that contains an SQL injection. The IDS will analyze the data when capturing packets.

```
--------------------------------------------------------------------------
GET /vehicleTracker.php?vehicleID=12345';DELETE+FROM+traffic_signals
+WHERE+1=1;--&action=view HTTP/1.1

Host: smarttransport.example.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8

Accept-Language; en-US,en;q=0.9

Connection: keep-alive
--------------------------------------------------------------------------
```

Figure 3: A sample SQL injection attempt on a car

It shows an HTTP request where a malicious user attempts an SQL injection by manipulating a URL parameter. The attacker targets the system's vehicle tracking page or traffic signal management interface with two parameters: `vehicleID` and `action`. The `vehicleID` parameter is set to `12345; DELETE FROM traffic_signals WHERE 1 = 1; -`, which attempts to alter the SQL query and delete all entries in the `traffic_signals` table. The `action` parameter is set to `view`, indicating the intention to display vehicle details after the malicious query is executed. By injecting the SQL command `DELETE FROM traffic_signals WHERE 1 = 1;`, and since the condition `1 = 1` always evaluates to true, a successful attack would delete all rows from the `traffic_signals` table.

4.2 Potential Impact of the Attack

In a smart transportation system, the traffic signals table might store critical information about the state of traffic lights across a city. If this table is deleted, it could result in traffic lights going offline or malfunctioning, leading to traffic chaos or accidents. Additionally, if the attack succeeds, it could also disrupt the vehicle tracking system, preventing authorities from monitoring the location and status of vehicles within the transportation network.

4.3 Extraction of Signature Data in the BIDST Framework for Blockchain Storage

Table 4 presents the structured signature data, extracted in accordance with the proposed BIDST framework, and prepared for secure storage in the blockchain. Each element provides essential information required for accurate detection, response, and long-term traceability.

Table 4: Detected attributes of the attack as per the BIDST framework

Tag	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
Meta data	Signature ID: 10123	Name: SQL injection attempt	Severity: high.	Category: web application attack	Revision number: 1	Source context: V2V
Description	Summary: identifies SQL injection attempts in HTTP requests by detecting suspicious patterns commonly used in SQL-based attacks.	Target systems: web servers and application servers	NA	NA	NA	NA
Conditions	Pattern/Rule: presence of common SQL injection signatures such as "1=1 –" within the HTTP request payload.	Payload content: NA	Header information: HTTP method is either POST or GET	Anomalous behavior: NA	Timing: repeated similar requests within a short time frame.	Contextual information: NA
Actions	Alert: generate a high-severity log entry and notify the Security Operations Center (SOC).	Response: temporarily block the offending IP address for 30 min	Logging: record full HTTP request details along with response codes.	NA	NA	NA
Examples	Matching traffic: a GET request containing parameters with the string "1=1 –"	False positives: ensure legitimate queries resembling SQL injection patterns are properly whitelisted	NA	NA	NA	NA
References	Documentation: OWASP SQL Injection Guide: https://owasp.org/www-community/attacks/ (accessed on 23 October 2025) SQLInjection	CVE IDs: CVE-2020-26623: SQL Injection in Web Application	NA	NA	NA	

(Continued)

Table 4 (continued)

Tag	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
Additional Information	Attack vector: typically executed via user input fields in web applications.	Mitigation strategies: implement prepared statements and parameterized queries to prevent SQL injection.	NA	NA	NA	NA

4.4 Smart Contract for Saving Signatures in Blockchain

Now we execute the smart contract to store the signature of attack in the blockchain. Fig. 4 shows the output of the successful execution of the smart contract. We can note the transaction cost and gas required for saving a single signature in the blockchain.

Figure 4: Successful execution of smart contract

4.5 Discussion

The rapid advancement of smart transportation systems necessitates robust security measures to protect critical infrastructure from cyber threats. Traditional signature-based IDS has long been employed to safeguard these systems, but it faces limitations in the face of increasingly sophisticated attacks. Blockchain technology, with its decentralized and immutable nature, offers a promising enhancement to these traditional systems. In this section we explore the effectiveness of traditional signature-based IDS against the proposed BIDST framework, focusing on security, efficiency, scalability, data integrity, cost, resilience against attacks, and regulatory compliance. Table 5 presents a comparison between the proposed approach and the traditional signature-based IDS.

Table 5: Comparison of traditional signature-based IDS and proposed BIDST IDS for smart transportation

Criteria	Traditional signature-based IDS	Proposed BIDST IDS
Security	Centralized architecture can become a single point of failure.	Decentralized verification enhances security, ensuring resilience against zero-day attacks. Immutability guarantees data integrity and reliable forensic analysis.
Efficiency	Fast detection for known threats but prone to high false positives, especially in complex environments.	Slightly slower due to consensus mechanisms, but achieves higher accuracy with reduced false positives, validated by multiple nodes.
Scalability	Difficult to scale in large transportation networks because of centralized processing constraints.	Better scalability through decentralized design, though it requires additional resources and infrastructure to support the network.
Data integrity	Vulnerable to tampering and manipulation in centralized systems, compromising audit trails.	Immutable blockchain records ensure data integrity, preventing tampering and providing trustworthy audit trails for investigations.
Cost	Lower initial and operational costs due to minimal infrastructure requirements.	Higher setup and operational costs from distributed infrastructure and increased computational demand.
Resilience against attacks	Less resilient against advanced attacks targeting central system availability or integrity.	Highly resilient to diverse cyberattacks, strengthened by its decentralized and immutable architecture.
Regulatory compliance	May face compliance challenges, particularly in data integrity and traceability requirements.	Facilitates compliance with regulations due to transparent, immutable records supporting auditability and reporting.

In Fig. 5, we have created a radar chart for comparing the performance metrics of traditional IDS vs. blockchain-based IDS across different parameters. By looking at the chart, it is evident that the blockchain based signature IDS has covered a large area, which means it has a better performance across the measured parameters. This allows us to visually analyze and present the effectiveness of traditional and blockchain based IDS systems in smart transportation. We can see that in two criteria, i.e., cost and efficiency the proposed framework's performance might be less than the traditional approach. This is because of the fact that as the number of nodes (which in our case represents the number of vehicles in the smart network) grow, the overhead of maintaining the blockchain grows rapidly. Blockchain-based intrusion detection systems, while offering decentralization, transparency, and immutability, inevitably introduce performance trade-offs due to consensus mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). These mechanisms increases computational and communication overhead. In terms of cost, for smart transportation systems, where IoT-enabled vehicles and roadside units may have limited hardware capacity, this overhead directly translates into infrastructure costs for additional processing and storage resources. In terms of efficiency, the requirement for multiple nodes to validate an intrusion signature update can lead to latency in detection and response time, particularly under real-time traffic scenarios. High verification delays

may reduce the IDS's ability to provide timely alerts. Furthermore, large-scale deployment across urban transportation networks amplifies the efficiency challenges due to increased synchronization traffic among blockchain nodes. However, there are some ways in which we can try to balance these trade-offs like using permissioned blockchains (to reduce the number of validators), lightweight consensus algorithms tailored for IoT/vehicular systems (e.g., RAFT, DPoS), and hybrid architectures where critical real-time detection is handled locally by agents while blockchain ensures secure logging and auditability.

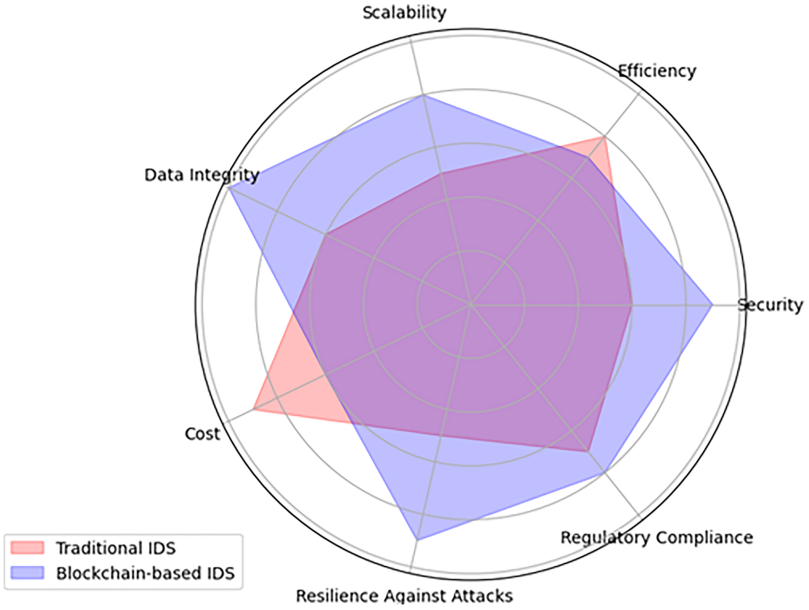

Figure 5: Comparison of signature-based IDS and blockchain-based IDS

5 Conclusion and Future Work

In this research, we proposed a framework for a signature-based intrusion detection system integrated with blockchain technology for enhancing the security of smart transportation systems. With the increasing adoption of intelligent transportation solutions, the need for robust, scalable, and secure communication frameworks has become critical. Traditional intrusion detection methods, while effective in some scenarios, face challenges in adapting to the decentralized and dynamic nature of smart transportation networks. We devised a method for storing the signatures of known attacks and wrote a smart contract for storing the signatures in blockchain. With the help of a case study, we showed how the usage of blockchain makes sure that the intrusion detection process is tamper-resistant, transparent, and auditable, thereby significantly reducing the risk of attacks such as tampering, man-in-the-middle, and unauthorized access. We then discussed the limitations of traditional IDS for smart transportation and how the usage of blockchain provides improved resilience against attacks, enhanced data integrity, and a more secure communication framework.

The current approach is based on signature-based intrusion detection but for enhanced security for the detection of unknown and emerging threats, we can include the anomaly-based detection that will result in a hybrid intrusion detection system. Within this integration, the signature-based component would continue to provide precise identification and classification of known attacks, ensuring low false positives, while the anomaly-based component would leverage statistical and machine learning techniques to flag deviations from normal traffic patterns, thereby detecting novel or zero-day threats.

Acknowledgement: Not applicable.

Funding Statement: This work was supported by the National Research Foundation (NRF), Republic of Korea, under project BK21 FOUR (4299990213939).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Hanaa Nafea, Awais Qasim, and Sana Abdul Sattar; Methodology, Hanaa Nafea, Awais Qasim, Sana Abdul Sattar, and Adeel Munawar; Software, Hanaa Nafea, Awais Qasim, and Sana Abdul Sattar; Validation, Awais Qasim, Adeel Munawar, and Muhammad Nadeem Ali; Formal Analysis, Sana Abdul Sattar, Adeel Munawar, and Byung-Seo Kim; Investigation, Sana Abdul Sattar, Adeel Munawar, and Muhammad Nadeem Ali; Resources, Awais Qasim, Muhammad Nadeem Ali, and Byung-Seo Kim; Data Curation, Hanaa Nafea, Awais Qasim, and Sana Abdul Sattar; Original Draft Preparation, Hanaa Nafea, Awais Qasim, and Sana Abdul Sattar; Rreview and Editing, Awais Qasim, Muhammad Nadeem Ali, and Byung-Seo Kim; Visualization, Hanaa Nafea, Awais Qasim, and Sana Abdul Sattar; Supervision, Awais Qasim and Byung-Seo Kim; Project Administration, Awais Qasim and Byung-Seo Kim; Funding Acquisition, Byung-Seo Kim. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated or analyzed during the current study are available in https://nvd.nist.gov/ (accessed on 23 October 2025).

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Supplementary Materials: The supplementary material is available online at https://www.techscience.com/doi/10.32604/cmc.2025.072281/s1.

References

1. Paul A, Ganguli I, Bhowmick RS, Badotra S, Bharany S, Rehman AU. DRL based traffic signal control method featuring masked approach to redress transmission error in ITS. Int J Intell Trans Syst Res. 2025;23(2):774–93. doi:10.1007/s13177-025-00482-z.
2. Ahmed U, Nazir M, Sarwar A, Ali T, Aggoune EHM, Shahzad T, et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Sci Rep. 2025;15(1):1726. doi:10.1038/s41598-025-92132-3.
3. Ali MN, Imran M, Din MSu, Kim BS. Low rate DDoS detection using weighted federated learning in SDN control plane in IoT network. Appl Sci. 2023;13(3):1431. doi:10.3390/app13031431.
4. Zhang C, Khan WU, Bashir AK, Dutta AK, Rehman AU, Al Dabel MM. Sum rate maximization for 6g beyond diagonal RIS-assisted multi-cell transportation systems. IEEE Trans Intell Trans Syst. 2025;26(10):17601–11. doi:10.1109/tits.2024.3521196.
5. Haider A, Adnan Khan M, Rehman A, Rahman M, Seok Kim H. A real-time sequential deep extreme learning machine cybersecurity intrusion detection system. Comput Mater Contin. 2021;66(2):1785–98. doi:10.32604/cmc.2020.013910.
6. Raza M, Barket AR, Rehman AU, Rehman A, Ullah I. Mobile crowdsensing based architecture for intelligent traffic prediction and quickest path selection. In: 2020 International Conference on UK-China Emerging Technologies (UCET); 2020 Aug 20–21; Glasgow, UK. New York, NY, USA: IEEE; 2020. p. 1–4.
7. Aloqaily M, Otoum S, Al Ridhawi I, Jararweh Y. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. 2019;90(4):101842. doi:10.1016/j.adhoc.2019.02.001.
8. Qasim A, Bilal M, Munawar A, Rehman Baig SU. Blockchain based intrusion detection in agent-driven flight operations. Multiagent Grid Syst. 2024;20(2):161–83. doi:10.3233/mgs-240017.
9. Nafea H, Qasim A, Hussain A, Fakhir I. Blockchain-based reputation model for vehicle platooning with common global goal. Multiagent Grid Syst. 2025;21(1):21–37. doi:10.1177/15741702251338060.
10. Farooq MS, Abbas S, Atta-Ur-Rahman, Sultan K, Khan MA, Mosavi A. A fused machine learning approach for intrusion detection system. Comput Mater Contin. 2023;74(2):2607–23. doi:10.32604/cmc.2023.032617.

11. Liao HJ, Lin CHR, Lin YC, Tung KY. Intrusion detection system: a comprehensive review. J Netw Comput Appl. 2013;36(1):16–24. doi:10.1016/j.jnca.2012.09.004.
12. Li W, Tug S, Meng W, Wang Y. Designing collaborative blockchained signature-based intrusion detection in iot environments. Future Gener Comput Syst. 2019;96(3):481–9. doi:10.1016/j.future.2019.02.064.
13. Winanto EA, Idris MY, Stiawan D, Nurfatih MS. Designing consensus algorithm for collaborative signature-based intrusion detection system. Indones J Electr Eng Comput Sci. 2021;22(1):485–96. doi:10.11591/ijeecs.v22.i1.pp485-496.
14. Abubakar AA, Liu J, Gilliard E. An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. Electron Lett. 2023;59(18):e12888. doi:10.1049/ell2.12888.
15. Kumar M, Singh AK. Distributed intrusion detection system using blockchain and cloud computing infrastructure. In: 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184); 2020 Jun 15–17; Tirunelveli, India. New York, NY, USA: IEEE; 2020. p. 248–52.
16. Sani MS, Iranmanesh S, Salarian H, Raad R, Jamalipour A. Bids: blockchain-enabled intrusion detection system in smart cities. IEEE Int Things Magaz. 2024;7(2):107–13. doi:10.1109/iotm.001.2300191.
17. Abdel-Basset M, Moustafa N, Hawash H, Razzak I, Sallam KM, Elkomy OM. Federated intrusion detection in blockchain-based smart transportation systems. IEEE Trans Intell Transp Syst. 2021;23(3):2523–37. doi:10.1109/tits.2021.3119968.
18. Krishna AM, Tyagi AK. Intrusion detection in intelligent transportation system and its applications using blockchain technology. In: 2020 International Conference on Emerging Trends in Information Technology and Engineering (IC-ETITE); 2020 Feb 24–25; Vellore, India. New York, NY, USA: IEEE; 2020. p. 1–8.
19. Ajayi O, Cherian M, Saadawi T. Secured cyberattack signatures distribution using blockchain technology. In: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC); 2019 Aug 1–3; New York, NY, USA. p. 482–8.
20. Golomb T, Mirsky Y, Elovici Y. Ciota: collaborative iot anomaly detection via blockchain. arXiv:1803.03807. 2018.
21. Signorini M, Pontecorvi M, Kanoun W, Di Pietro R. Bad: a blockchain anomaly detection solution. IEEE Access. 2020;8:173481–90. doi:10.1109/access.2020.3025622.
22. Kolokotronis N, Brotsis S, Germanos G, Vassilakis C, Shiaeles S. On blockchain architectures for trust-based collaborative intrusion detection. In: 2019 IEEE world congress on services (SERVICES); 2019 Jul 8–13; Milan, Italy. Vol. 2642. New York, NY, USA: IEEE; 2019. p. 21–8. doi: 10.1109/services.2019.00019.
23. Alexopoulos N, Vasilomanolakis E, Ivánkó NR, Mühlhäuser M. Towards blockchain-based collaborative intrusion detection systems. In: Critical Information Infrastructures Security: 12th International Conference, CRITIS 2017; 2017 Oct 8–13; Lucca, Italy. Cham, Switzerland: Springer; 2018. p. 107–18.