International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March – 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Design and Development of Security Model for IOT Based Smart Transportation System

Rajesh Piplode, Research Scholar, SAGE University Indore (MP) India
Dr. Sanjay Singh Bhadoriya, Associate Professor, SAGE University Indore (MP) India

Abstract: The integration of Internet of Things (IoT) technologies into intelligent transportation systems has become a key enabler for smart cities, supporting real-time traffic management, connected vehicles, and enhanced public safety. However, the highly distributed and heterogeneous nature of IoT-based smart transportation environments introduces significant security and privacy challenges, including device impersonation, data tampering, denial-of-service attacks, and cyber-physical threats that can directly impact human safety.

This research paper presents a layered security model for IoT-enabled smart transportation systems, designed using a defense-in-depth approach. The proposed model addresses security requirements across multiple layers, including the perception layer, communication network, edge/fog layer, cloud infrastructure, and in-vehicle systems. Key security mechanisms such as secure boot, public key infrastructure–based authentication, end-to-end encryption, secure V2X communication, intrusion detection systems, role-based access control, and secure over-the-air updates are incorporated to ensure confidentiality, integrity, availability, and system resilience.

In addition, the model emphasizes privacy preservation through data anonymization, trust and identity management and incident response strategies to maintain safe operation under attack conditions. The proposed framework is scalable, real-time capable, and adaptable to evolving threat landscapes, making it suitable for large-scale smart city deployments. This work provides a comprehensive foundation for securing future intelligent transportation systems against both cyber and cyber-physical attacks.

Keywords: IoT Security, Smart Transportation, Intelligent Transportation Systems, V2X Communication, Cyber-Physical Security, Smart Cities.

1. Introduction

An IoT-based Transportation System is an advanced intelligent transportation framework that leverages the Internet of Things (IoT), cyber-physical systems, and data analytics to enable real-time monitoring, control, and optimization of transportation networks. The system consists of interconnected sensing devices, embedded controllers, communication modules, and cloud-based platforms that collectively acquire, transmit, process, and analyze large volumes of transportation-related data.

In this system, various sensors such as GPS modules, RFID, LiDAR, ultrasonic sensors, cameras, and environmental sensors are deployed in vehicles and roadside infrastructure to collect parameters including vehicle speed, location, traffic density, road conditions, and emissions. Communication technologies such as Wi-Fi, cellular networks (4G/5G), Dedicated Short-Range Communication (DSRC), and LPWAN protocols enable reliable data transmission between vehicles (V2V), vehicles and infrastructure (V2I), and cloud servers.

The collected data is processed using cloud computing and edge computing architectures, where machine learning and data analytics algorithms are applied for traffic prediction, congestion management, route optimization, and anomaly detection. Real-time decision-making allows dynamic traffic signal control, automated incident detection, fleet tracking, and predictive vehicle maintenance [1].

IoT-based transportation systems improve operational efficiency, enhance road safety, reduce energy consumption, and support sustainable mobility. They form a critical component of Intelligent Transportation Systems (ITS) and play a key role in enabling smart mobility solutions and autonomous transportation within smart city ecosystems.

2. Security Model Summary Diagram

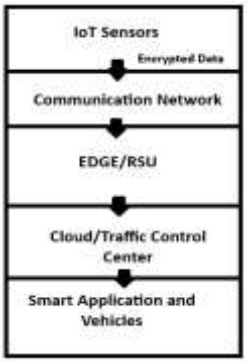

Fig 1. IoT transportation flowchart diagram

Fig 1. Shows IoT transportation flowchart diagram. IoT sensors collect real-time traffic and environmental data and send it securely in encrypted form through the communication network. Edge/RSU units process this data locally to reduce latency and support fast decisions, then forward relevant information to the cloud or traffic control center for large-scale analysis. The processed insights are finally delivered to smart applications and connected vehicles to enable safe, efficient, and intelligent transportation services.

3. Security Threat Analysis (Potential System Risks)

An IoT-based smart transportation system is exposed to a wide range of security threats due to its distributed architecture, heterogeneous devices, and reliance on wireless communication. Device spoofing and impersonation can occur when attackers mimic legitimate sensors, vehicles, or roadside units to inject false data into the system. Data tampering, such as manipulation of traffic flow or sensor readings, can lead to incorrect traffic signal control, congestion, or unsafe routing decisions. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks can disrupt communication networks or cloud services, causing system unavailability and delays in real-time operations.

Additionally, unauthorized access to vehicle systems or traffic management infrastructure may allow attackers to control or disable critical functions. Privacy leakage is a major concern, as continuous data collection can expose sensitive information such as vehicle identity, travel patterns, and real-time location of users. Malware and firmware attacks targeting IoT devices can compromise system integrity, enable persistent backdoors, or spread across the network. Furthermore, Man-in-the-Middle (MitM) attacks can intercept and alter communication between vehicles, roadside units, and control centers, leading to false commands or data corruption. Collectively, these threats highlight the need for robust security mechanisms in IoT-based transportation systems [2].

4. Layered Security Model (Defense in Depth)

Layer	Security Goals	Mechanisms
Perception Layer (IoT Devices & Sensors)	Confidentiality, Integrity, Device Authenticity [3]	Secure boot & hardware root of trust Device authentication using certificates (PKI) Lightweight encryption (AES-128/256) Physical tamper resistance Firmware integrity checks & signed updates
Communication Layer (Network & Data Transmission)	Secure data transmission & availability	End-to-end encryption (TLS/DTLS) Secure V2X protocols (IEEE 1609.2) VPN tunnels for RSUs and edge nodes Network segmentation & firewalls Anti-jamming and DoS detection mechanisms
Edge/Fog Layer (Roadside Units & Local Controllers)	Low-latency secure processing	Mutual authentication between devices and RSUs Intrusion Detection Systems (IDS) Secure containerization (Docker, trusted execution

		environments) Role-based access control (RBAC)
Cloud / Application Layer	Data security, analytics integrity, system availability[4]	Strong access control (RBAC / ABAC) Encrypted databases and backups Secure APIs with OAuth 2.0 Continuous monitoring and SIEM Regular penetration testing
Vehicle Security Layer	Vehicle safety & passenger protection	Secure CAN bus gateways ECU authentication Over-the-air (OTA) updates with code signing Isolation of infotainment and control systems

Table 1. Layered Security Model

4.1 Perception Layer (IoT Devices & Sensors)

The perception layer in an IoT-based transportation system consists of IoT devices and sensors that collect real-time data from vehicles and road infrastructure, such as speed, location, traffic density, and environmental conditions. The primary security goals of this layer are to ensure that sensed data is reliable, protected from unauthorized access, and originates from legitimate devices. Since this layer directly interacts with the physical environment, it is vulnerable to device compromise, data manipulation, and identity misuse. Achieving strong security at the perception layer is essential to maintain trust in the collected data and to support safe and accurate operation of higher layers within the transportation system [3].

4.1.1 Perception Layer Security Goals

(1) Confidentiality

In an IoT-based transportation system, confidentiality refers to the protection of sensitive transportation-related information from unauthorized access. This includes data such as vehicle locations, traffic patterns, driver details, and communication between vehicles and traffic infrastructure. If confidentiality is compromised, attackers may gain access to private or strategic transportation data, leading to privacy violations, surveillance, or misuse of system information.

(2) Integrity

Integrity ensures that the data exchanged within the transportation system remains accurate, consistent, and trustworthy. Transportation systems rely heavily on real-time data for decision-making, and any unauthorized modification of traffic data, vehicle status information, or control messages can result in incorrect traffic management, unsafe driving conditions, or system malfunction.

(3) Device Authenticity

Device authenticity refers to the assurance that all participating entities in the transportation system—such as vehicles, sensors, roadside units, and control systems—are genuine and authorized. A lack of device authenticity can allow malicious or fake devices to join the network, inject false information, or disrupt transportation operations.

4.1.2 Techniques to achieve security goals of physical layer:

(i) Secure boot & hardware root of trust

Secure boot and hardware root of trust refer to the foundational security concepts that ensure an IoT or transportation device starts its operation in a trustworthy state. Secure boot focuses on verifying that only authorized and unmodified firmware is executed when a device powers on, while the hardware root of trust represents the most reliable and tamper-resistant component of the system that serves as the basis for establishing trust. Together, they form the starting point of device trust, helping ensure that the system begins execution from a known, legitimate state and maintains overall system reliability [5].

(ii) Device authentication using certificates (PKI)

In an IoT-based transportation system, device authentication using certificates ensures that only legitimate vehicles, sensors, roadside units (RSUs), and control devices can participate in the network. As see in figure 2 each device is assigned a unique digital certificate issued by a trusted Public Key Infrastructure (PKI) authority. Before exchanging data, the device presents its certificate, which is verified by other network entities to confirm its authenticity. This process prevents spoofing, unauthorized access, and malicious device injection, ensuring that traffic data, vehicle control commands, and communication between vehicles and infrastructure remain trustworthy and secure. Certificate-based authentication is especially critical in connected and autonomous vehicles, where real-time decisions depend on the integrity and authenticity of device communications [6].

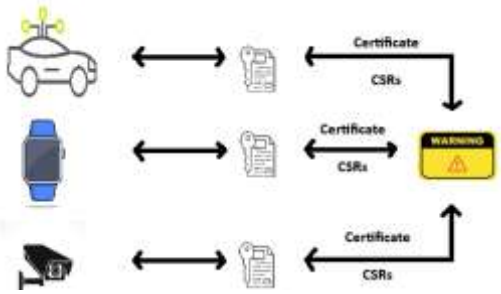

Fig. 2 Device authentication using certificates

(iii) Lightweight encryption (AES-128/256)

In an IoT-based transportation system, data generated by vehicles, roadside units, and sensors is often sensitive, including vehicle locations, traffic patterns, and control commands. In figure 3 it shows lightweight encryption, such as AES (Advanced Encryption Standard) with 128-bit or 256-bit keys, is used to protect this data while minimizing computational and energy overhead, which is important for resource-constrained IoT devices. AES ensures that transmitted data remains confidential and secure from eavesdropping or unauthorized access, even over wireless networks. Using lightweight encryption allows real-time communication between vehicles, traffic management systems, and control centers without compromising system performance, making it a critical component for secure and reliable smart transportation systems [7].

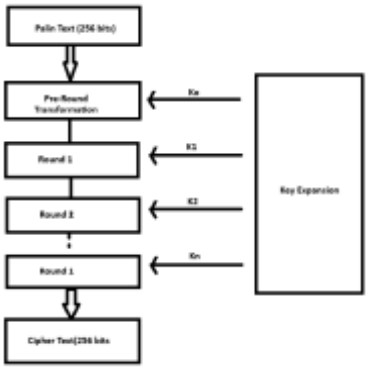

Fig. 3 Lightweight encryption (AES-128/256)

(iv) Physical tamper resistance

Tamper resistance and physical attacks target secure hardware by exploiting weaknesses at the physical level. These attacks are broadly classified into non-invasive, semi-invasive, and invasive attacks. Non-invasive attacks do not physically damage the device and usually leave no evidence; they include timing attacks, power analysis, electromagnetic analysis, glitch attacks, and data remanence exploitation. Such attacks rely on observing variations in execution time, power consumption, electromagnetic emissions, or residual data in memory to extract secret information like cryptographic keys and passwords. They are relatively low-cost and highly effective, especially against poorly implemented cryptographic systems.

In contrast, invasive and semi-invasive attacks involve partial or full physical access to the chip. Invasive attacks require decapsulation, microprobing, laser cutting, focused ion beam (FIB) modification, and reverse engineering,

often leaving clear tamper evidence but allowing deep access to internal signals and memory. Semi-invasive attacks bridge the gap by using techniques such as UV exposure, infrared imaging, laser fault injection, and backside probing without direct electrical contact. The study concludes that defending against physical attacks requires multi-layered protection, continuous reassessment of threats, and a strong understanding of evolving attack technologies by hardware security designers.

To defend against non-invasive attacks, systems should use constant-time algorithms to prevent timing leaks, balanced and masked cryptographic operations to reduce power and electromagnetic leakage, and noise generation or random delays to obscure side-channel signals. Secure key management is critical: keys should be generated randomly, stored securely, frequently refreshed, and never kept in SRAM without protection. Voltage, clock, and temperature sensors can detect abnormal conditions and trigger resets or data erasure to counter glitch and fault attacks. Proper PCB design, shielding, and internal voltage regulation further reduce susceptibility to power and EM analysis.

For invasive and semi-invasive attacks, hardware-level protections are essential. These include tamper-detecting meshes, active shields, encrypted internal buses, and sensors for light, UV, and physical probing. Sensitive memory should be protected with encryption, redundancy, and automatic zeroization upon tamper detection. Using modern fabrication technologies with multiple metal layers, backside protection, and obfuscation makes reverse engineering significantly harder. Overall, effective defense requires layered security—combining hardware, software, and physical safeguards—and continuous updates as attack techniques evolve [8].

(v) Firmware integrity checks & signed updates

Firmware integrity checks and signed updates are essential for securing IoT transportation systems such as connected vehicles, traffic controllers, and roadside units. Firmware integrity checks use cryptographic hashes to verify that the firmware stored on a device has not been altered, while digital signatures ensure that only updates issued by an authorized authority are accepted. During boot and update processes, the device validates the firmware signature using a securely stored public key, preventing malicious code injection and unauthorized firmware modification that could compromise safety-critical transportation operations.

In IoT transportation systems, signed firmware updates also protect against downgrade and replay attacks by enforcing version control and rollback prevention. Secure update delivery over encrypted channels, combined with secure boot and tamper-resistant key storage, ensures system reliability even in hostile network environments. Together, these mechanisms help maintain trust, safety, and resilience across large-scale, distributed transportation infrastructures [9].

4.2 Communication Layer (Network & Data Transmission)

The Communication Layer in an IoT-based Smart Transportation System is responsible for enabling data transmission between various components such as vehicles, sensors, traffic signals, roadside units, control centers, and cloud platforms. It acts as a bridge between the perception layer (which collects data through sensors and devices) and the application layer (which processes data and provides services like traffic monitoring and route optimization). This layer ensures reliable, real-time, and secure communication across the entire transportation network.

The communication layer uses both short-range and long-range network technologies depending on the application. Short-range communication technologies such as Wi-Fi (802.11p/DSRC), Bluetooth, Zigbee, and RFID are used for close-distance communication like vehicle-to-vehicle (V2V) and electronic toll collection. Long-range communication technologies such as 4G/5G cellular networks, NB-IoT, LTE-M, LoRaWAN, and satellite communication are used for wide-area connectivity, real-time vehicle tracking, and smart parking systems. These technologies allow continuous data exchange even across large geographic areas.

Different communication models are supported within this layer, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Cloud (V2C). These models enable vehicles to share information about speed, location, traffic conditions, and road hazards. Lightweight communication protocols such as MQTT and CoAP are commonly used to ensure efficient data transmission, while HTTP/HTTPS, TCP/UDP, and IPv6 support web connectivity and large-scale device addressing.

Security is a critical aspect of the communication layer. Techniques such as encryption (TLS/SSL), device authentication, secure key management, and intrusion detection systems are implemented to protect data from cyber

threats. Overall, the communication layer plays a vital role in ensuring real-time traffic management, reducing congestion, preventing accidents, and improving the overall efficiency and safety of smart transportation systems [10].

4.2.1 Communication Layer Security Goals

(i) Secure data transmission: Secure data transmission ensures that information exchanged between IoT devices, vehicles, roadside units, and servers is protected from unauthorized access and modification.
(ii) Availability: ensures that communication services and data in an IoT-based transportation system remain accessible and operational whenever required, especially for real-time and safety-critical applications [4].

4.2.2 Techniques to achieve security goals of Communication Layer

(i) End-to-end encryption (TLS/DTLS)

End-to-end encryption using TLS/DTLS plays a vital role in securing communication in IoT-based smart transportation systems. It ensures that data transmitted between IoT devices such as vehicles, sensors, roadside units, and backend servers remains protected from unauthorized access throughout the entire communication path. Transport Layer Security (TLS) is commonly used for secure and reliable communication, particularly in vehicle-to-cloud interactions and traffic management servers. Datagram Transport Layer Security (DTLS), on the other hand, is designed for low-latency and unreliable networks and is well suited for vehicle-to-vehicle and sensor communications using UDP. This encryption mechanism protects sensitive information such as vehicle location, speed, traffic status, and control commands. It effectively prevents security threats including eavesdropping, man-in-the-middle attacks, replay attacks, and data tampering. By ensuring confidentiality, integrity, and authentication, TLS/DTLS allows secure data exchange without exposing information to intermediate nodes. Additionally, lightweight DTLS variants support the real-time and resource-constrained requirements of smart transportation systems [11].

(ii) Secure V2X protocols

As show in figure 4 secure V2X communication in IoT-based smart transportation systems is enabled through IEEE 1609.2, which defines security services for vehicular communication. This standard provides mechanisms for authentication, integrity, and confidentiality of messages exchanged between vehicles (V2V), roadside units (V2I), and infrastructure networks. IEEE 1609.2 uses digital certificates, public key infrastructure (PKI), and cryptographic techniques to ensure that only trusted vehicles and devices participate in communication. It protects safety-critical messages such as collision warnings, speed alerts, and traffic signal information from spoofing, replay, and message modification attacks. By securing V2X communication, IEEE 1609.2 enhances trust, reliability, and safety in real-time smart transportation environments[6].

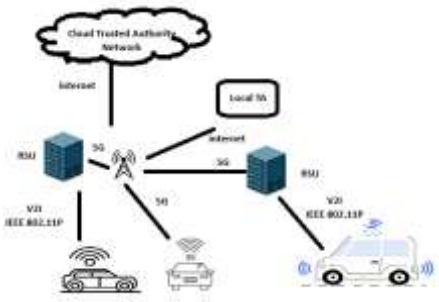

Fig. 4 Secure V2X protocols

(iii) VPN tunnels for RSUs and edge nodes

As show in figure 5 VPN tunnels are used to securely connect roadside units (RSUs) and edge nodes in an IoT-based transportation system over public or untrusted networks. These tunnels create an encrypted communication channel that protects traffic data, sensor information, and control messages from unauthorized access. VPN technologies such as IPsec or TLS-based VPNs ensure confidentiality by encrypting data before transmission and decrypting it only at the authorized endpoints. They also provide authentication to verify the identity of RSUs and edge nodes and maintain data integrity during transmission. By encapsulating communication within secure tunnels,

VPNs prevent eavesdropping, data tampering, and man-in-the-middle attacks. This secure connectivity improves reliability, supports continuous data availability, and enables safe coordination between RSUs, edge nodes, and central traffic management systems [12].

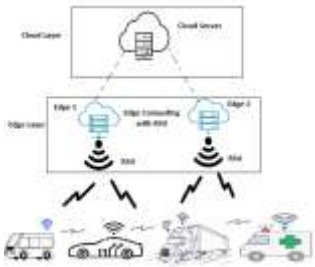

Fig. 5 VPN tunnels for RSUs and edge nodes

(iv) Network segmentation & firewalls

Network segmentation and firewalls are essential security mechanisms in an IoT-based transportation system to protect communication infrastructure from cyber threats as show in figure 6. Network segmentation divides the overall network into smaller, isolated segments such as vehicle networks, roadside units, edge nodes, and backend servers. This limits unauthorized access and prevents the spread of attacks across the entire system. Firewalls are deployed between these segments to monitor and control incoming and outgoing traffic based on predefined security rules. They block malicious traffic, unauthorized connections, and suspicious data packets. Together, network segmentation and firewalls enhance system security by reducing the attack surface, enforcing access control, and ensuring secure and reliable data transmission within smart transportation environments.

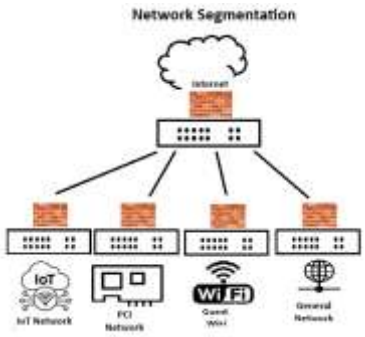

Fig. 6 Network segmentation & firewalls

(v) Anti-jamming and DoS detection mechanisms

Anti-jamming and Denial-of-Service (DoS) detection mechanisms are critical for maintaining availability in IoT-based transportation systems. Anti-jamming techniques protect wireless communication between vehicles, sensors, and roadside units by detecting and mitigating intentional interference in the communication channels. Methods such as frequency hopping, spread spectrum communication, and adaptive power control help ensure reliable data transmission even under jamming attacks. DoS detection mechanisms continuously monitor network traffic to identify abnormal patterns such as excessive packet requests or sudden traffic spikes that may indicate an attack. Once detected, mitigation strategies such as traffic filtering, rate limiting, and rerouting are applied to maintain continuous network operation. Together, these mechanisms enhance communication reliability, prevent service disruption, and ensure the availability of safety-critical transportation services [2,6] .

4.3 Edge/Fog Layer (Roadside Units & Local Controllers)

The Edge/Fog Layer in an IoT-based Smart Transportation System consists of roadside units (RSUs), local controllers, gateways, and edge computing devices that process data close to where it is generated. This layer is positioned between the communication layer and the cloud layer, and its primary function is to reduce latency by performing real-time data processing at the network edge. Instead of sending all raw data to the cloud, the edge/fog

layer filters, analyzes, and makes quick decisions locally, which is essential for time-critical transportation applications.

Roadside Units (RSUs) are installed along roads, intersections, and highways to communicate directly with vehicles and traffic sensors. They support Vehicle-to-Infrastructure (V2I) communication and collect data such as vehicle speed, traffic density, accident alerts, and environmental conditions. Local controllers manage traffic signals, smart parking systems, surveillance cameras, and digital signboards. These controllers can automatically adjust traffic light timing based on congestion levels detected by nearby sensors.

The edge/fog layer improves system efficiency by reducing network bandwidth usage, minimizing communication delays, and enhancing reliability. For example, if an accident occurs, the roadside unit can instantly alert nearby vehicles without waiting for cloud processing. It also ensures continued operation even if cloud connectivity is temporarily lost. Additionally, security measures such as local authentication, data encryption, and firewall protection are implemented at this layer to protect sensitive transportation data.

Overall, the Edge/Fog Layer plays a crucial role in enabling fast decision-making, real-time traffic control, reduced congestion, and improved safety in IoT-based smart transportation systems.

4.3.1 Edge/Fog Layer Security Goals

In an IoT-based transportation system, the edge/fog layer consists of roadside units (RSUs) and local controllers that perform real-time data processing close to vehicles and sensors. The primary security goal of this layer is to ensure low-latency secure processing of safety-critical information such as collision warnings, traffic signal control, and congestion updates. By processing data locally, the edge/fog layer reduces dependence on cloud communication and minimizes response time. Security mechanisms such as device authentication, secure boot, encrypted communication, and access control are implemented without introducing significant delays. Lightweight encryption and intrusion detection techniques are used to protect data integrity and confidentiality while meeting strict real-time requirements. This combination of local processing and security ensures fast, reliable, and secure decision-making in smart transportation systems.

4.3.2 Mechanisms

(i) Mutual authentication between devices and RSUs

Mutual authentication between IoT devices and roadside units (RSUs) is essential to establish trust and secure communication in smart transportation systems. In this process, as show in figure 7 both the device (such as a vehicle or sensor) and the RSU verify each other's identity before exchanging data. Cryptographic techniques such as digital certificates, public key infrastructure (PKI), and challenge–response mechanisms are commonly used to prevent unauthorized or malicious devices from accessing the network. Mutual authentication protects the system from spoofing, impersonation, and replay attacks while ensuring that only legitimate entities participate in communication. By confirming the authenticity of both ends, it enables secure and reliable data exchange with minimal delay, supporting real-time transportation applications[13].

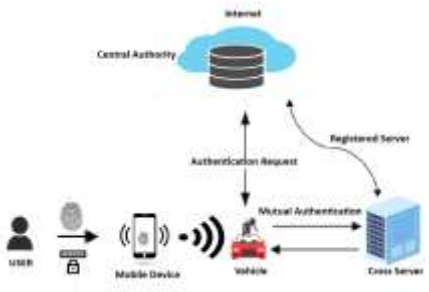

Fig. 7 Mutual authentication between devices and RSUs

(ii) Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are critical for monitoring and protecting IoT-based transportation networks from malicious activities. In below figure 8 IDS continuously analyze network traffic and system behavior at the edge, roadside units (RSUs), and local controllers to detect anomalies, suspicious patterns, or known attack signatures. They can identify threats such as unauthorized access, data tampering, Denial-of-Service (DoS) attacks, and malware infiltration. IDS can be signature-based, which compares activities against a database of known attacks, or anomaly-based, which detects deviations from normal behavior. Upon detection, IDS can trigger alerts, log events, or initiate automated mitigation actions, such as isolating affected nodes or rerouting traffic. By providing real-time threat detection and response, IDS enhance the security, reliability, and resilience of smart transportation systems[14].

Fig. 8 Intrusion Detection Systems (IDS)

(iii) Secure containerization (Docker, trusted execution environments)

Secure containerization is an effective method to isolate and protect applications running on edge/fog nodes, roadside units (RSUs), and local controllers in IoT-based transportation systems. Technologies like Docker allow services and applications to run in lightweight, isolated containers, preventing faults or attacks in one container from affecting others. Additionally, Trusted Execution Environments (TEEs) provide hardware-based secure areas within processors, ensuring that sensitive operations—such as cryptographic computations, authentication, and traffic data processing—are executed in a protected environment. Together, these approaches enhance security by ensuring data confidentiality, integrity, and isolation, while supporting low-latency, reliable, and secure processing of real-time transportation information.

(iv) Role-based access control (RBAC)

Role-Based Access Control (RBAC) is a security mechanism used to regulate access to resources in IoT-based smart transportation systems based on user or device roles. As figure 9 show in this system, each entity—such as vehicles, roadside units (RSUs), edge nodes, or administrators—is assigned a specific role with predefined permissions. For example, a vehicle may have permission to send telemetry data, an RSU may have permission to control traffic signals, and an administrator may have full network management rights. RBAC ensures that entities can only perform actions allowed by their role, preventing unauthorized access, data manipulation, and misuse of system resources. By enforcing least-privilege principles, RBAC enhances security, accountability, and operational reliability across the edge/fog layer of smart transportation networks[15].

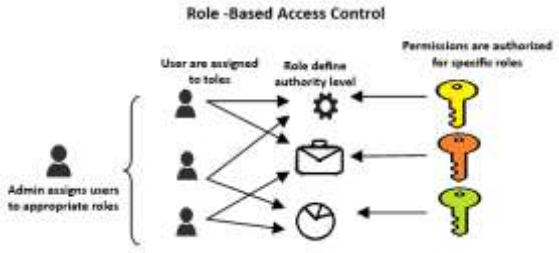

Fig. 9 Role-based access control

4.4 . Cloud / Application Layer

The Cloud / Application Layer in an IoT-based Smart Transportation System is the topmost layer of the architecture, responsible for large-scale data storage, advanced data processing, analytics, and service delivery to end users. This layer receives data from the edge/fog layer and communication layer, where it is stored in cloud servers and processed using big data analytics, artificial intelligence (AI), and machine learning (ML) algorithms. The cloud layer enables centralized monitoring and management of the entire transportation network.

One of the key functions of this layer is data analysis and decision support. It analyzes traffic patterns, predicts congestion, detects accidents, and optimizes routes in real time. Historical data stored in the cloud helps authorities plan infrastructure improvements, manage public transport schedules, and reduce fuel consumption and emissions. The cloud also supports smart services such as dynamic route guidance, smart parking management, fleet tracking, and emergency response systems.

The application layer provides user interfaces such as mobile apps, web dashboards, and control center systems. Traffic authorities can monitor live traffic conditions, adjust signal timings remotely, and generate reports. Drivers and passengers can access real-time traffic updates, estimated arrival times, parking availability, and navigation assistance through mobile applications.

Security and data management are critical in this layer. Cloud platforms implement strong authentication, encryption, backup systems, and disaster recovery mechanisms to ensure data safety and system reliability. Overall, the Cloud / Application Layer plays a vital role in intelligent decision-making, system-wide coordination, and delivering smart transportation services efficiently and effectively.

4.4.1 Cloud / Application Layer Security Goals

The cloud or application layer in an IoT-based smart transportation system handles large-scale data storage, advanced analytics, and decision-making for traffic management, route optimization, and safety monitoring. The primary security goals at this layer include data security**,** analytics integrity, and system availability. Data security ensures that sensitive information, such as vehicle telemetry, passenger details, and traffic patterns, is protected against unauthorized access and breaches through encryption, access control, and secure APIs. Analytics integrity guarantees that the processing and analysis of this data are accurate and tamper-proof, preventing malicious manipulation that could affect traffic decisions or automated responses. System availability ensures that cloud services remain reliable and accessible, even under high traffic load or cyber-attacks, supporting real-time and continuous operation of smart transportation applications. Together, these security goals protect the system against data breaches, manipulation, and service disruption, maintaining trust and reliability across the transportation network.

4.4.2 Mechanisms

(i) Strong access control (RBAC / ABAC)

Strong access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), are essential for securing the cloud and application layer of IoT-based smart transportation systems. RBAC assigns permissions based on predefined roles, ensuring that users, devices, or services can only perform actions authorized for their role—for example, a traffic controller can update signal timings, while a vehicle can only send telemetry data. ABAC provides finer-grained access by evaluating attributes such as time, location, device type, or operational context before granting access. These mechanisms prevent unauthorized access, reduce the risk of data breaches, and enforce least-privilege policies. By combining RBAC and ABAC, cloud systems can ensure that sensitive data, analytics functions, and system operations are accessed securely and appropriately, maintaining the confidentiality, integrity, and availability of transportation services[15]. In below table shows RBAC and ABAC criteria base comparison.

Criteria	RBAC	ABAC
Access	Based on the role	Based on attribute
Flexibility	Limited (for Small and midsized)	Yes

Scalability	Moderate	High
Effectiveness	Effective if there is a clear role hierarchy that determines data access	High effective at defining data access
Implementation	Easy to establish' but hard to maintain while the number of roles increases	Requires time and specialized skills to establish' but easy to maintain

Table 2. RBAC and ABAC Criteria comparison

(ii) Encrypted databases and backups

Encrypted databases and backups are essential for protecting sensitive data stored and processed in the cloud layer of IoT-based smart transportation systems. Vehicle telemetry, passenger information, traffic analytics, and control commands are stored in databases that are encrypted using strong cryptographic algorithms, such as AES or RSA, ensuring confidentiality even if the storage medium is compromised. Backups of these databases are also encrypted and securely stored, providing protection against data loss, ransomware attacks, or unauthorized access. Encryption ensures that only authorized cloud services or users with proper decryption keys can access the data, maintaining the integrity and confidentiality of critical transportation information. This approach guarantees that real-time analytics, decision-making, and historical records remain secure and reliable, supporting safe and efficient transportation operations.

(iii) Secure APIs with OAuth 2.0

Secure APIs are crucial for enabling controlled and safe communication between IoT devices, edge nodes, and cloud services in smart transportation systems. OAuth 2.0 is an industry-standard authorization framework that allows applications to access resources on behalf of users or devices without exposing credentials. By issuing access tokens with specific scopes and lifetimes, OAuth 2.0 ensures that only authorized devices or applications can access sensitive data, such as vehicle telemetry, traffic analytics, or route information. This prevents unauthorized access, data leakage, and API misuse while supporting scalable and secure integration of multiple services. Combined with HTTPS/TLS, OAuth 2.0 enables secure, authenticated, and fine-grained access control for APIs in real-time transportation applications, maintaining the confidentiality, integrity, and availability of system data.

(iv) Continuous monitoring and SIEM

Continuous monitoring and Security Information and Event Management (SIEM) systems are critical for maintaining the security, integrity, and availability of cloud services in IoT-based smart transportation systems. Continuous monitoring involves real-time tracking of network traffic, device activity, application logs, and cloud resource usage to detect anomalies, potential threats, or system failures. SIEM platforms aggregate and correlate logs and events from multiple sources, such as vehicles, edge nodes, and cloud applications, to provide comprehensive visibility and enable rapid detection of cyberattacks, misconfigurations, or performance issues. Alerts generated by SIEM allow administrators to respond quickly with mitigation actions, such as isolating compromised components, blocking suspicious traffic, or initiating automated recovery procedures. Together, continuous monitoring and SIEM enhance situational awareness, support proactive threat detection, and ensure the reliability and resilience of smart transportation services.

(v) Regular penetration testing

Regular penetration testing is a proactive security practice used to identify vulnerabilities and weaknesses in cloud applications, APIs, databases, and network infrastructure of IoT-based smart transportation systems. Ethical hackers or automated tools simulate real-world attacks, such as unauthorized access attempts, injection attacks, or misconfigured cloud services, to assess the system's resilience against cyber threats. By performing penetration tests periodically, organizations can discover security gaps before malicious actors exploit them and apply necessary patches,

configuration changes, or updates. This process helps maintain the confidentiality, integrity, and availability of transportation data and services while ensuring compliance with security standards. Regular penetration testing strengthens the overall security posture of smart transportation platforms, making them more robust against evolving cyberattacks.

5. Vehicle Security Layer

The Vehicle Security Layer in an IoT-based Smart Transportation System is responsible for protecting vehicles and their internal systems from cyber threats, unauthorized access, and data breaches. As modern vehicles are equipped with IoT sensors, GPS modules, onboard units (OBUs), and communication systems that connect to external networks, they become vulnerable to hacking, malware, spoofing, and other cyberattacks. The vehicle security layer ensures the confidentiality, integrity, and availability of vehicle data and control systems.

This layer secures communication between the vehicle and external entities such as other vehicles (V2V), roadside infrastructure (V2I), pedestrians (V2P), and cloud platforms (V2C). It uses encryption techniques such as TLS/SSL to protect transmitted data and implements strong authentication mechanisms to verify the identity of devices and users. Digital certificates and secure key management systems are commonly used to prevent unauthorized access.

Inside the vehicle, security mechanisms protect critical components like the Electronic Control Units (ECUs), Controller Area Network (CAN bus), infotainment systems, and autonomous driving modules. Firewalls, intrusion detection systems (IDS), secure boot mechanisms, and firmware update authentication help prevent malicious software from compromising vehicle functions. Regular over-the-air (OTA) updates are also securely managed to fix vulnerabilities and improve system security.

The Vehicle Security Layer plays a crucial role in ensuring passenger safety, preventing vehicle hijacking, safeguarding personal data, and maintaining trust in smart transportation systems. By implementing strong cybersecurity measures, this layer helps create a secure and reliable connected vehicle ecosystem[14, 16].

5.1 Vehicle Security Layer Security Goals

The vehicle security layer focuses on ensuring the safety of vehicles and protection of passengers in IoT-based smart transportation systems. This layer integrates security mechanisms within vehicles, including onboard sensors, control units, and communication modules, to safeguard against cyberattacks, unauthorized access, and system malfunctions. Key security goals include protecting vehicle control systems (such as braking, steering, and engine management) from tampering, securing in-vehicle communications (V2V, V2X), and safeguarding passenger data collected by infotainment or telematics systems. Techniques such as intrusion detection systems for in-vehicle networks, secure boot, encrypted communications, and regular software updates help maintain the integrity and reliability of vehicle operations. By achieving these goals, the vehicle security layer ensures safe, reliable transportation and minimizes risks to passengers from both cyber threats and system failures.

5.2 Mechanisms

(i) Secure CAN bus gateways

Secure CAN bus gateways play a critical role in protecting in-vehicle communication networks from cyber threats. The Controller Area Network (CAN) bus connects various electronic control units (ECUs) within a vehicle, such as engine control, braking, and infotainment systems. Without security, CAN buses are vulnerable to message spoofing, replay attacks, and unauthorized control commands. Secure CAN bus gateways enforce message authentication, integrity checks, and filtering, ensuring that only legitimate messages are transmitted between ECUs. They may also implement encryption for sensitive commands and isolate critical systems from less-trusted modules. By securing the CAN bus, these gateways protect vehicle operations from cyberattacks, prevent malicious manipulation of critical systems, and contribute to the overall safety of passengers and vehicle integrity.

(ii) ECU authentication

ECU authentication ensures that only legitimate Electronic Control Units (ECUs) within a vehicle can communicate over in-vehicle networks such as the CAN bus. Each ECU is assigned a unique identity and cryptographic credentials, allowing it to authenticate itself before sending or receiving critical control messages.

Authentication mechanisms prevent unauthorized or malicious ECUs from injecting harmful commands into the vehicle systems, protecting components such as braking, steering, engine control, and infotainment. Techniques such as digital signatures, challenge–response protocols, and secure key management are commonly used to verify ECU identities. By enforcing strict authentication, vehicles maintain the integrity and reliability of in-vehicle communications, reduce the risk of cyberattacks, and ensure passenger safety.

(iii) Over-the-air (OTA) updates with code signing

As show in Figure 10 over-the-air (OTA) updates with code signing are essential for securely maintaining and upgrading vehicle software in IoT-based smart transportation systems. OTA updates allow manufacturers to remotely deploy software patches, firmware upgrades, and security fixes to vehicles without requiring a service visit. Code signing ensures that the updates are digitally signed by a trusted source, allowing the vehicle to verify the authenticity and integrity of the code before installation. This prevents attackers from injecting malicious firmware or tampering with updates, which could compromise critical systems such as braking, steering, or engine management. By combining OTA delivery with code signing, vehicles maintain secure and reliable operations, protect against cyberattacks, and ensure passenger safety while keeping vehicle software up-to-date.

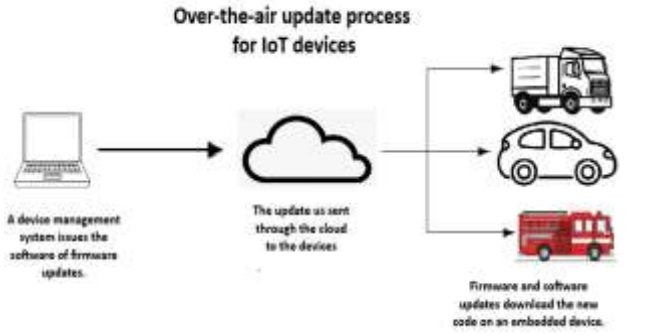

Fig. 10 Over-the-air (OTA) updates with code signing

(iv) Isolation of infotainment and control systems

Isolation of infotainment and control systems is a critical security measure in IoT-based smart vehicles to protect safety-critical operations and passenger data. Infotainment systems, which handle media, navigation, and connectivity features, are often exposed to external networks such as the internet or mobile devices, making them potential entry points for cyberattacks. By isolating these systems from control networks that manage critical vehicle functions—such as braking, steering, and engine management—vehicles prevent malware or unauthorized access in the infotainment system from affecting safety-critical operations. Techniques such as hardware partitioning, virtual LANs (VLANs), and firewalls within the vehicle network ensure this separation. This isolation enhances vehicle security, maintains operational integrity, and ensures passenger safety even if the infotainment system is compromised.

5. Future Work

While the proposed security model offers comprehensive protection for IoT-based smart transportation systems, several research directions remain open for future exploration:

1. AI-Driven Security Mechanisms

Future work can integrate machine learning and artificial intelligence techniques for advanced anomaly detection, predictive threat analysis, and adaptive intrusion response, particularly at the edge and vehicle layers.

2. Zero Trust Architecture (ZTA)

Extending the model with Zero Trust principles—continuous authentication, least-privilege access, and contextual trust evaluation—can further reduce insider threats and lateral movement attacks.

3. Blockchain-Based Trust and Data Integrity

Blockchain and distributed ledger technologies can be explored for decentralized trust management, secure V2X message validation, and tamper-proof logging without relying on centralized authorities [17].

4. Post-Quantum Cryptography

As quantum computing advances, future research should investigate lightweight post-quantum cryptographic algorithms suitable for resource-constrained IoT and vehicular devices.

5. Standardization and Interoperability

Further work is needed to align security mechanisms across heterogeneous devices and vendors by mapping the model more deeply to standards such as ISO 21434, IEEE 1609, NIST IoT Framework, and ETSI ITS.

6. Real-World Deployment and Performance Evaluation

Large-scale pilot implementations and simulations can be conducted to evaluate the model's impact on latency, scalability, energy consumption, and real-time responsiveness in smart city environments.

6. Conclusion

The rapid adoption of IoT-based smart transportation systems has transformed urban mobility by enabling real-time traffic management, connected vehicles, and intelligent public transit. However, this increased connectivity also expands the attack surface, exposing transportation infrastructures to cyber and cyber-physical threats that can directly impact public safety, privacy, and system availability.

This work presented a layered security model for IoT-enabled smart transportation environments, addressing security challenges across the perception, communication, edge/fog, cloud, and vehicle layers. By integrating mechanisms such as device authentication, end-to-end encryption, secure V2X communication, access control, intrusion detection, and secure OTA updates, the proposed model ensures confidentiality, integrity, availability, and safety throughout the system lifecycle.

In addition, the model emphasizes privacy preservation**,** trust and identity management, and resilience, which are critical for large-scale smart city deployments. The defense-in-depth approach ensures that even if one layer is compromised, the overall system remains protected and capable of operating in fail-safe modes. Overall, this security framework provides a scalable and practical foundation for securing modern intelligent transportation systems against evolving threats.

7. Reference

1. Sergi, I.; Montanaro, T.; Benvenuto, F.L.; Patrono, L. A Smart and Secure Logistics System Based on IoT and Cloud Technologies. Sensors 2021, 21, 2231. https://doi.org/ 10.3390/s21062231
2. Sanaz Hami Hassan Kiyadeh , Hamiden Abd El-Wahed Khalifa, "Designing Secure-by-Design IoT for Smart Transportation: A Privacy-Aware Data Analytics," Smart City Insights Vol. 2, No. 3 (2025) 125–135
3. Muhammad Awais Javed, Elyes Ben Hamida and Wassim Znaidi, "Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice" Sensors 2016, 16, 879; doi:10.3390/s16060879.
4. H. Karthikeyan, G. Usha, "A secured IoT-based intelligent transport system (IoT-ITS) framework based on cognitive science" Soft Computing https://doi.org/10.1007/s00500-023-08410-7
5. Rashmi R V, Karthikeyan A, "Secure boot of Embedded Applications – A Review" Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018) IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1
6. Thomas Kothmayr, Corinna Schmitt , Wen Hu , Michael Brunig and Georg Carle, "A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication" 7th IEEE International Workshop on Practical Issues in Building Sensor Network Applications 2012, SenseApp 2012, Clearwater, Florida
7. Sabri, O.; Al-Shargabi, B.; Abuarqoub, A.; Hakami, T.A. A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. IoT 2025, 6, 23. https://doi.org/10.3390/ iot6020023
8. Dr Sergei Skorobogatov, "Tamper resistance and physical attacks ", ECRYPT-2006 Summer School on Cryptology Louvain-la-Neuve, Belgium, 12-15 June 2006
9. Saad El Jaouhari , Eric Bouvet, "Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions" Internet of Things Volume 18, May 2022, 100508, https://doi.org/10.1016/j.iot.2022.100508
10. Srinivas Jangirala, Ashok Kumar Das, Mohammad Wazid, and Athanasios V. Vasilakos, "Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System IEEE Internet of Things Journa, DOI 10.1109/JIOT.2020.3040938

11. Martina Brachmann, Sye Loong Keoh, Oscar Garcia Morchon and Sandeep S. Kumar, "End-to-End Transport Security in the IP-based Internet of Things", 21st International Conference on Computer Communications and Networks (ICCCN) 2012 https://10.1109/ICCCN.2012.6289292
12. N. M. Saravana Kumar, S. Balamurugan, Hari K. Prasath, A, " A Novel Cyber-Security Approach for Nodal Authentication in IoT Using Dual VPN Tunneling", Cyber-Physical Systems and Industry 4.0, Apple Academic Press, 1st Edition, 2022
13. Lo, N.-W.; Huang, J.-J.; Yang, T.-C. A Lightweight Mutual Authentication Mechanism for Applications Utilizing Low-Power IoT Devices. Electronics 2025, 14, 4178. https://doi.org/10.3390/ electronics14214178
14. E. Biermann, E.Cloete, L.M. Venter, "A comparison of Intrusion Detection systems", Computers & Security, Vol. 20, No. 8 (2001) 676-683
15. Jaibir Singh , Suman Rani , Vipin Kumar, "Role-Based Access Control (RBAC) EnabledSecureandEfficient Data Processing Framework for IoTNetworks" International Journal of Communication Networks and InformationSecurity 2024, 16(2), 6623 ISSN: 2073-607X,2076-0930 https://https://ijcnis.org/
16. Weerasinghe, N.; Usman, M.A.; Hewage, C.; Pfluegel, E.; Politis, C. Threshold Cryptography-Based Secure Vehicle-to-Everything (V2X) Communication in 5G-Enabled Intelligent Transportation Systems. Future Internet 2023, 15, 157. https:// doi.org/10.3390/fi15050157
17. Yi Yang, Debiao He , Pandi Vijayakumar , Brij B. Gupta , and Qi Xie, "An Efficient Identity-Based Aggregate Signcryption Scheme With Blockchain for IoT-Enabled Maritime Transportation System", IEEE Transactions on green communications and networking, vol. 6, no. 3, september 2022