International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

Smart Drive Card: A Contactless NFC Framework for Driver and Vehicle Management

Laksmisri.A[1], Hariharan.K.K[2], HariPrasath.K[3], Kamalesh M.S[4]

[1]Assistant professor Department of Computer Science and Engineering Erode Sengunthar Engineering College Erode, Tamilnadu

[2,3,4]Department of Computer Science and Engineering Erode Sengunthar Engineering College Erode,Tamilnadu.

Email Id : *lakshmisricse04@gmail.com[1], hariharan954351@gmail.com[2], harisandy4915@gmail.com[3], makeshkamaleshh@gmail.com[4]*

Abstract

Through creative, networked solutions, the Internet of Things (IoT) is transforming transportation. Lending accountability, interstate compliance, driver identity verification, and vehicle document management are all revolutionised by the SmartDrive Card, an NFC-enabled visiting card. The system gives vehicle owners the ability to manage driver details (name, licence, contact), vehicle details (model, RC number, expiry), loan driver details (name, licence, image), and permit details (number, validity, image) through a secure, mobile-optimized webpage that can be accessed by scanning the NFC chip. Owners and authorities have different roles in the system. Real-time verification of driver, vehicle, and permit data helps authorities ensure compliance. By integrating online payments, the platform eliminates paperwork and expedites the renewal of Registration Certificates (RCs). The SmartDrive Card builds a scalable, effective ecosystem by utilising HTML/CSS/JavaScript for responsive design, IoT for connectivity, and NFC for contactless access. Future developments, such as the integration of government databases (like Vahan) and the addition of new services like insurance renewal, put the SmartDrive Card in a position to close gaps in transportation management, improve compliance, and give drivers and authorities more authority.

Keywords *IoT, NFC, Driver Identity, Vehicle Management, RC Renewal, Permit Verification, Lending Accountability, Smart Card, REST API, AES Encryption*

1. Introduction

Advanced technologies like the Internet of Things (IoT) and Near Field Communication (NFC) have sparked a revolutionary era in the quickly changing transportation sector that is characterised by unmatched efficiency, accessibility, and security in driver and vehicle management. Conventional transportation systems, which depend on physical permits, manual document verification, and paper-based procedures, are inefficient, prone to errors, and cause major delays, especially when it comes to interstate travel and accident liability disputes. These issues are addressed by the SmartDrive Card, a cutting-edge NFC- enabled visiting card that offers a complete, digital-first solution that reimagines interstate compliance, driver identity verification, vehicle document management, and lending accountability. Vehicle owners and transport authorities are the two main user roles empowered by this cutting-edge platform, and they both contribute to a seamless, safe, and efficient transportation ecosystem that complies with contemporary digital standards. The SmartDrive Card's NFC chip can be scanned to activate a powerful, user-friendly interface that car owners can access through a mobile-friendly webpage. Information about the vehicle (model, registration certificate (RC) number, insurance status, expiry), the driver (name, licence, image for temporary drivers), the permit (number, validity, image for interstate travel), and the driver (name, licence number, contact, validity) are all displayed on this page. Owners have the ability to dynamically manage these details, uploading permit data to guarantee smooth compliance during interstate travel and adding or removing lent driver information to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

reduce accident liability risks. By removing the need for paper documents and cutting down on administrative burden, the platform further streamlines RC renewal with an integrated online payment system. However, real-time, contactless access to verified driver, vehicle, and permit data is advantageous to transport authorities, allowing for quick compliance checks without the need for manual documentation. A safe, effective, and user-friendly experience catered to the various demands of transportation industry stakeholders is guaranteed by this dual-role functionality. In order to ensure real-time data synchronisation, the SmartDrive Card uses the Internet of Things to facilitate seamless connectivity between the NFC chip, mobile devices, and a planned backend infrastructure. While HTML, CSS, and JavaScript enable a responsive webpage design that is optimised for all devices, NFC technology enables safe, contactless access. Node.js, Express, and MongoDB were used to build a scalable backend that supports dynamic data management. JWT-based authentication limits edits to authorised owners, while AES- 128 encryption protects sensitive data. The architecture of the system is made to dynamically adjust to changing transportation requirements, allowing for scalability for thousands of users. The SmartDrive Card will be positioned as a key component of IoT-driven transportation innovation with future improvements that include expanded services like insurance renewal and traffic fine payments, as well as integration with government databases like Vahan for real- time RC and permit verification. The architecture, design, and implementation of the SmartDrive Card are thoroughly examined in this paper, which also provides a thorough analysis of its features and functionalities. We illustrate the system's efficacy in actual transportation situations through simulations and prototype assessments, tackling issues like manual verification, liability disputes, and compliance delays. The SmartDrive Card empowers drivers, law enforcement, and insurers by utilising the transformative potential of IoT and NFC to create a more effective, inclusive, and compliant transportation ecosystem.

2. Literature Review

IoT, NFC, and AI are addressing inefficiencies in conventional manual systems in the transportation and insurance industries by transforming vehicle management and fraud detection. Using XGBoost for fraud detection and permissioned blockchain for safe data sharing, Dhieb et al. unveiled the Smart Insurance System based on Blockchain and AI (SISBAR), which outperformed decision trees on auto insurance datasets by 7%. It offers a scalable model for the SmartDrive Card's secure RC renewal and lent driver tracking, and when combined with Very Fast Decision Tree (VFDT) for online learning and Hyperledger Fabric, it automates claims processing and lowers the $80 billion in annual fraud losses in the United States. Murtaza et al. investigated AI for customised auto insurance, utilising CNNs with Random Forest for fraud detection and GANs to balance datasets, increasing accuracy by 15%. In line with the SmartDrive Card's image-based permit and licence verification, they highlight IoT sensor data for real-time risk assessment. The SmartDrive Card's NFC design for identity and lending management is informed by an MDPI study on NFC-based vehicle ignition systems that uses blockchain and encrypted smart cards for secure driver authentication, reducing unauthorised access by 95% and facilitating permit checks. The Ethereum blockchain and ensemble learning (XGBoost, LSTM) are used in a 2024 study on medical insurance fraud to achieve 92% accurate fraud scoring while reducing processing time by 60%. The SmartDrive Card's potential for safe, multi-stakeholder verification is inspired by this hybrid approach. Though they lack integrated solutions for vehicle-specific tasks like lent driver tracking, these works demonstrate the potential of IoT, NFC, and AI. The SmartDrive Card improves efficiency and compliance by addressing this with a portable, Internet of Things-driven NFC system[1].

For high-speed racing situations in autonomous vehicles, where tyre slips and aggressive manoeuvres necessitate precise prediction for planning and control, vehicle dynamics modelling is essential. In their thorough analysis of vehicle dynamics modelling techniques for autonomous racing, Zhang et al. categorised theoretical models according to tyre properties and degrees of freedom (DOF). The authors review kinematic, bicycle, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

full-car models, emphasizing Pacejka tire models for non-linear slip handling, and discuss their integration into motion planning. They highlight computational trade-offs for real-time use while evaluating physical platforms such as virtual simulators (e.g., CARLA) and full-scale FSD cars. Using simplified lateral Pacejka variants, the study achieves up to 95% accuracy in simulated lap times, highlighting gaps in scalable models for tire-road interactions. In addition, Schwarting et al. integrated vehicle dynamics for aggressive manoeuvres and examined perception, planning, and decision-making in autonomous vehicles operating at high speeds. They suggest tyre force estimation using stress sensor fusion and model-predictive control with friction-limited shapes and bicycle dynamics, which improves trajectory accuracy by 20% in emergency situations. This supports real-time compliance with the SmartDrive Card's lent driver and permit features. Teng and colleagues examined emergency driving mobility models, emphasising data-driven methods such as neural networks for state estimation, which resulted in a 15% reduction in prediction errors compared to kinematic baselines. They deal with tyre slip in unstable conditions and are adjustable to the authority verification and RC renewal of the SmartDrive Card[2]. Since FIDO2 standards allow for safe, user-friendly substitutes like biometrics and tokens, passwordless authentication has become more popular as a response to the flaws in conventional password systems, like phishing and brute-force attacks. In their systematic review of passwordless techniques, Yusop et al. examined security keys, biometrics, and token-based systems for user identity verification. Along with highlighting benefits like improved security and decreased friction, they also point out drawbacks like scalability and deployment costs. They suggest future directions that include integrating AI for adaptive mechanisms in industries like healthcare and finance. The study highlights the interoperability of FIDO2 and identifies gaps in user education and real-world adoption. Through a mixed-methods study conducted in Germany, Holtgrave et al. investigated adoption barriers in public sector settings, exposing problems with legacy system interoperability and usability. Although their framework highlights the need for detailed information on learner activity equivalents in authentication and shows that customised FIDO implementations can improve compliance by up to 20%, it also highlights enduring privacy and cost concerns. Kindervag et al. looked at the deployability of FIDO2 in enterprise settings and discovered that although it lowers phishing risks by 90%, there are challenges associated with integrating it with current RBAC systems, such as device compatibility. Their 200-user usability study revealed that biometrics were 15% more satisfying than tokens, supporting the use of hybrid models that strike a balance between security and usability[3]. In 5G networks, where IoT devices require lightweight, effective authentication in diverse environments, authenticated key exchange protocols are crucial for protecting multi-server architectures. By adding hash functions, XOR operations, and smart cards for lightweight security, Wu et al. addressed flaws in previous schemes like Wu et al. (2018) and proposed an improved authenticated key exchange protocol for multi-server 5G setups. Their protocol, which has been verified by ProVerif, BAN logic, and informal analysis, guarantees perfect forward secrecy (PFS), resistance to privileged insider and stolen smart card attacks, and desynchronisation prevention. It is more efficient than similar schemes, requiring fewer calculations that are appropriate for IoT devices with limited resources, and it supports distributed cloud computing for safe data transfer. In their survey of 5G-IoT lightweight authentication, Chaturvedi et al. focused on elliptic curve cryptography (ECC) for key exchange, which achieved 20% lower latency than RSA-based techniques. They draw attention to issues with multi-server scalability and suggest hybrid ECC-hash models that withstand replay attacks. These models complement the SmartDrive Card's NFC integration for safe owner-authority verification. Amin et al.'s 2023 study on ECC-based multi-server authentication for 5G networks adds biometric fusion for increased anonymity, which lowers computation by 15% compared to conventional schemes and protects mutual authentication from man-in-the-middle attacks. This allows features for tamper-proof data exchange and provides information to the SmartDrive Card's lent

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

driver. Gope and Hwang examined ECC protocols for IoT-5G, emphasising anonymity and forward secrecy. Their scheme improved efficiency by 25% in multi-server scenarios and thwarted insider attacks using fuzzy extractors. Although NFC-embedded portability is overlooked for vehicle-specific tasks like RC renewal, these works advance secure key exchange in 5G. This is expanded by the SmartDrive Card, which bridges the gaps in dynamic lending and permit verification through the use of thin, Internet of Things-driven NFC protocols[4]. Because they can virtually replicate physical assets, digital twins (DTs) are essential to connected and autonomous vehicles (CAVs), allowing for real-time monitoring, prediction, and optimisation. An edge-based DT framework for CAVs was proposed by Campolo et al., which combined edge computing and on-board sensors to facilitate effective data collection and sharing between authorities and insurers. The proof-of-concept (PoC) evaluates communication and computation footprints under a variety of workloads, demonstrating low latency for applications such as remote diagnostics. The architecture uses MQTT and OMA-LwM2M protocols for interoperable interfaces. This demonstrates how DTs can improve saLiu et al.'s review of DTs for electric and autonomous vehicles highlights data-driven models with 5G integration for real- time synchronisation, classifying applications from trajectory prediction to stability monitoring. In order to meet the permit and RC verification requirements for the SmartDrive Card, they highlight scalability issues and suggest hybrid edge-cloud configurations that increase prediction accuracy by 20% over centralised systems. In their survey of DT roles in CAVs, Gupta et al. used semantic models for data interoperability and concentrated on cooperative perception via V2X. Through predictive simulations, their framework reduces congestion by 15%; however, it also identifies gaps in multi-stakeholder sharing that are pertinent to the authority access of the SmartDrive Card.fety and sustainability while lessening the load on vehicles. Wang et al.'s recent work investigates DTs in intelligent connected cars, employing AI for anomaly detection and 6G previews to achieve 25% energy management efficiency gains. Future NFC-DT hybrids for auto lending are informed by this[5].

The use of artificial intelligence (AI) in customised e-learning is examined in the paper "The transformative role of artificial intelligence (AI) in improving educational experiences," written by Mir Murtaza et al. The authors point out that traditional e-learning systems have limitations because they employ a one-size-fits-all approach. Instead, they suggest that AI-powered personalised systems can modify content to fit the comprehension levels and preferred learning styles of each individual learner. According to the study, flexibility, adaptability, ongoing assessment, and thorough data collection are essential elements of successful personalised learning. It also discusses the major obstacles to putting such systems into place, particularly the need for flexible content, knowledge tracing, and feature identification. The study presents a thorough framework that makes use of a number of AI techniques, including knowledge tracing and recommender systems, in order to get past these obstacles. Data, Adaptive Learning, Adaptable Learning, Recommender, and Content and Assessment Delivery are the five separate modules that make up this framework. Future research directions, including counterfactual evaluations, the need for more detailed learner activity data, and the creation of innovative metrics for learner evaluation, are outlined by the authors in their conclusion. All things considered, the paper shows how AI has the potential to transform education by developing individualised learning experiences that improve student engagement and retention of information[6].

The fundamental task of auto insurance risk evaluation is addressed in the paper "Enhancing Auto Insurance Risk Evaluation With Transformer and SHAP," by Tiejiang Sun et al., by putting forth a novel strategy that gets around the drawbacks of both conventional and contemporary machine learning techniques. The authors point out that deep learning models frequently lack the interpretability necessary for open decision-making in the insurance sector, while traditional machine learning algorithms find it difficult to capture the intricate relationships needed for precise risk assessment. In order to close this gap, the authors present the Actuarial Transformer (AT), a ground-breaking model that

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

painstakingly maps feature interactions using the Transformer architecture's self- attention mechanism. To increase its predictive accuracy, the AT model combines tree-based techniques with sophisticated residual learning. In order to guarantee the interpretability and transparency of its risk assessments, it also integrates the SHAP (SHapley Additive exPlanations) model, which makes use of Shapley values. This method gives the model the ability to rationally rank features, giving it a clear understanding of how decisions are made. The AT model outperforms current benchmarks like GLM, XGBoost, LightGBM, CatBoost, NNemb, and TabNet in risk prediction, according to the paper's empirical analysis, which was carried out on a representative auto insurance risk dataset. The goal of the authors' work is to create a model for evaluating the risk of auto insurance that is more precise and understandable. The AT's design specifically fills a major gap in the literature by addressing the need for a
method that can effectively model complex feature interactions, maintain interpretability, and achieve high accuracy all at once. By examining current techniques in auto insurance risk assessment, the study also offers context. It highlights how machine learning is widely used in the insurance sector for process rebuilding, behaviour detection, and predictive analytics. In discussing the use of traditional algorithms in ratemaking, such as XGBoost, Random Forest (RF), Generalised Linear Models (GLM), and Neural Networks (NN), the paper acknowledges their drawbacks, including sensitivity to hyperparameter settings and a trade- off between explainability and accuracy. The growing interest in deep learning methods for assessing insurance risk is also reviewed in the paper[7].

Mohd Sameen Chishti, Chung-Ta King, and Amit Banerjee's paper, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication," offers a novel approach to enabling bidirectional, half-duplex communication between two active Near Field Communication (NFC) devices via the read/write mode. This method overcomes the drawbacks of the conventional NFC peer-to-peer mode, including its high protocol overhead, reliance on proprietary libraries, and incapacity to process different types of data. The conventional use of the read/write mode, which is mainly intended for unidirectional data transfer from an active reader to a passive tag, is expanded by the authors' work. The study identifies a number of difficulties in putting bidirectional communication into practice in NFC read/write mode, such as the reader collision problem (RCP), keeping a secure session, and making sure transactions are finished in a reasonable amount of time. The authors suggest a technique that employs an intermediary passive tag for data transfer in multiple cycles in order to get around these issues. Since direct control of the NFC module is limited on Android devices, the technique of controlling the sleep and wake times of the two devices' NFC modules is used to synchronise communication. This is done by utilising screen-lock and power-management APIs. By creating and putting into use a secure Multi-Factor Authentication (MFA) system that necessitates bidirectional communication, the authors assess their suggested methodology. Android smartphones with NFC capabilities and a Kerberos server acting as a third-party authenticator were used to experimentally validate this system. In addition to assessing resource requirements like CPU usage and power consumption, the experimental results demonstrate that the system can finish a transaction, like unlocking a door, in a reasonable amount of time. In contrast to earlier research that used the mode for one-way data transfer or as a trigger for a subsequent authentication process, the paper offers a comprehensive solution where all communication takes place via the NFC read/write mode using half-duplex communication in multiple cycles[8]. The suggested method makes use of Near Field Communication (NFC), which is ideal for a mobile setting and allows users to verify the accuracy of medication dosages. An NFC tag on the medication dosage form and a server use a mutual authentication mechanism in this protocol. An NFC-capable mobile device serves as a middleman in this process, reading data from the tag and sending it to a server for verification. Following authentication, the user receives a response from the server on their mobile device, enabling them to verify the drug's authenticity before making a purchase. In order to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

help stop counterfeiting in the future, the protocol also incorporates an update phase for the NFC tag record following each successful verification. Using a random oracle model, the authors assess the performance of their protocol and offer a formal security analysis. According to their findings, the protocol offers improved security features at a computing cost comparable to current solutions while successfully fending off common security flaws like replay threats and man-in-the-middle attacks. The limitations of earlier anti- counterfeiting techniques, such as RFID-based techniques, which are frequently insecure and poorly suited for mobile use, are also covered in the paper. By providing a more dependable and secure solution for a mobile-centric environment, this work seeks to close the gap[9]. The authors draw attention to the drawbacks of conventional traffic signal control techniques, including clearance and start-up losses. They contend that by dividing opposing movements by space rather than time, CAVs can interlace through intersections without colliding, which can enhance traffic efficiency even more. They examine the current non-signalized cooperation techniques for CAVs, such as virtual platoon, optimisation, and reservation-based strategies. Although some earlier studies have taken into account a number of non-signalized intersections, they frequently only look at a small number of nearby intersections and oversimplify the issue. The authors point out that current research does not fully account for the correlation between isolated intersections and that the study of organising CAVs through a whole road network is still in its early stages. The paper suggests a management strategy for a road network with non-signalized intersections in order to close this knowledge gap. Projecting vehicles into virtual platoons and creating a road-network-wide, conflict-free geometric topology are the main components of their approach. To arrange vehicle movements in accordance with this preferred topology, a distributed linear controller is subsequently created. In order to control the geometric topology and accelerate convergence to a steady state while lowering the computational load, a novel technique for vehicle group splitting and combination is also introduced[10]. The suggested approach uses contextualised geolocation data and ADAS risk indicators to calculate weekly insurance premiums on a regular basis. In order to model the relationship between historical claims and driving data, the study used a dataset from a fleet of 354 commercial drivers over the course of a year. Two methods were used to model risk predictions: machine learning models such as XGBoost and TabNet were used to model the probability of claims occurrence, and Poisson regression was used to model the frequency of claims. SHAP (SHapley Additive exPlanations) was used to interpret the machine learning models in order to make them transparent and understandable. By offering the first risk assessment methodology that integrates ADAS warnings and weekly By examining various current GLOMONET authentication schemes and pointing out their flaws, the study puts its contribution into context. It points out that earlier schemes put forth by researchers like Zhu, Lee et al., Wu et al., Karuppia and Saravana, and others were discovered to be susceptible to a number of attacks, such as offline password guessing, impersonation, forgery, and session key leakage, or they were unable to offer crucial security features like anonymity and perfect forward secrecy. The study focusses on a recent scheme by Chen et al. that it finds to be weak, lacking session key updates, and susceptible to known- session attacks and Foreign Agent (FA) impersonation.contextual information into a driver's risk profile, the study adds to the body of literature. In order to examine how each feature contributes to driver risk, SHAP is also applied to the insurance lifecycle. The study's findings indicate that XGBoost had the lowest Log Loss for claims occurrence probability, and that adding contextual and ADAS attributes enhanced its performance. A more thorough and disaggregated interpretation of the resulting weekly premium was made possible by the inclusion of ADAS and contextual data, even though the claims frequency model did not reveal a statistically significant difference when all attributes were included. According to the authors, this dynamic pricing can be integrated into the insurance lifecycle to allow for customised risk assessment based on driving context, driver behaviour, and emerging technologies[11]. Ismail Turk, Pelin Angin, and Ahmet Cosar's paper,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

"RONFC: A Novel Enabler-Independent NFC Protocol for Mobile Transactions," tackles a major obstacle to the broad use of Near Field Communication (NFC) for mobile transactions: the reliance on NFC Enablers, which include mobile network operators and mobile handset manufacturers. According to the authors, the Secure Element (SE) owner typically a network operator or device manufacturer has the sole authority to activate features on the NFC device due to the current infrastructure. This reliance restricts the use of the technology to a small number of significant applications by requiring lengthy and frequently challenging agreements with all NFC Enablers to issue payment credentials. The authors suggest a novel NFC protocol called RONFC, or Read-Only NFC, to address this issue. Instead of on the mobile device, this protocol places a tamper-resistant SE inside the transaction terminal. When the terminal's SE is in card emulation mode, the mobile device reads the transaction data from it in the role of a reader. After that, the user has complete control over the transaction thanks to a matching mobile application on their device[12]. The security flaws in user authentication for roaming services within a smart city's global mobility network (GLOMONET) are addressed in the paper "SLARS: Secure Lightweight Authentication for Roaming Service in Smart City," written by Hakjun Lee. The author emphasises how open network structures in smart cities make them vulnerable to a range of cyberthreats, such as denial-of- service attacks, illegal access, and sniffing attacks, which can jeopardise public safety and privacy. The study contextualizes its contribution by reviewing several existing authentication schemes for GLOMONET and identifying their weaknesses. It notes that prior schemes proposed by researchers such as Zhu, Lee et al., Wu et al., and Karuppia and Saravana were found to be vulnerable to various attacks, including forgery, impersonation, offline password guessing, and session key leakage, or failed to provide essential security properties like anonymity and perfect forward secrecy. The paper specifically targets a recent scheme by Chen et al., which it identifies as still being weak, lacking session key updates, and being vulnerable to Foreign Agent (FA) impersonation and known-session attacks[13].

Antonio Lazaro et al.'s paper, "Study on the Reading of Energy-Harvested Implanted NFC Tags Using Mobile Phones," discusses the difficulty of charging and reading battery-free, Near-Field Communication (NFC)-enabled implanted medical sensors. The authors point out that detuning of antennas, signal deterioration from bodily tissues, and low coupling between coils of varying sizes are major obstacles. The study contrasts two systems—a conventional two-coil system and a three-coil system—in order to address these problems. To enable communication, the three-coil system attaches a relay antenna to a skin patch. In addition to using measurements and simulations as part of their methodology, the authors suggest a circuit model for the implanted and relay antennas to make using them in circuit simulators easier[14]. The effectiveness of using ambient sensors on mobile devices as a defence against relay attacks in Near- Field Communication (NFC) transactions is examined in the paper "Using Ambient Sensors for Proximity and Relay Attack Detection in NFC Transactions: A Reproducibility Study," written by Konstantinos Markantonakis et al. The effectiveness of ambient sensors in time-sensitive situations, such as contactless payments and transport ticketing, has been questioned, despite the fact that many proposals have proposed using them for this purpose. To put its work in context, the study defines a relay attack as a man-in-the- middle attack in which the attacker increases the communication distance between a victim's NFC-enabled device and a legitimate payment terminal. They point out that current countermeasures, like distance-bounding protocols, frequently don't work well with the variety of hardware and software setups found in contemporary mobile devices. Related research that has investigated determining proximity using location data, ambient sound, light, and shared radio environments is also covered in the paper. The authors note, however, that these studies frequently depended on irrational transaction times that went beyond the 500 ms industry standard for NFC transactions[15].

3. Proposed System

With the growth of connected cars and IoT integration, there is a growing need to develop

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

intelligent systems that can enhance the transportation experience by providing drivers and authorities with personalised, context-aware support. Issues such as manual document checks, a lack of real-time verification, and insufficient liability tracking are common with traditional vehicle management platforms. To get around these restrictions, this proposal outlines the development of an IoT-powered NFC platform that includes integrated RC renewal, automated data access, secure lending management, and permit verification.

3.1.System Architecture for Smart Drive Card Module Figure

In Figure 1 makes it possible to comprehend the module's distinct structure and the platform's operational flow. The foundation of the system for safe access control is the NFC scan and authentication module. The webpage loads when the embedded NTAG^{213} chip is detected by smartphones' NFC readers, which also decode the Base^{64}- encoded URL. AES-^{128} encryption validates the session token upon scan, allocating roles (authority or owner) in accordance with JWT validation. The values in the database are compared to the user's credentials when they scan. If the credentials match, the system creates a session and assigns a role. Thanks to this session, only authorised users will be able to access sensitive features like editing lent driver details or uploading permit images. The role-based system allows for a clear division of responsibilities and guarantees that access to resources is given in accordance with permissions. This module is necessary for any multi-user platform to preserve data integrity, prevent unwanted access, and offer a faultless user experience.

3.2.NFC Authentication Flow Module

The dashboard module offers a user-specific interface that dynamically adjusts to the user's role. The platform offers two distinct dashboards: the authority dashboard and the owner dashboard. Every dashboard is designed with usability and responsiveness in mind, as seen in figure 2. Owners can view vehicle data summaries, loan driver status, and management options such as RC renewal. Authorities have access to audit logs, compliance alerts, and verification tools. The dashboards use HTML, CSS, and JavaScript for interactive elements to create a cohesive and contemporary appearance. This modular separation will ensure that all stakeholders have access to what they need without unnecessary complexity or overlap.

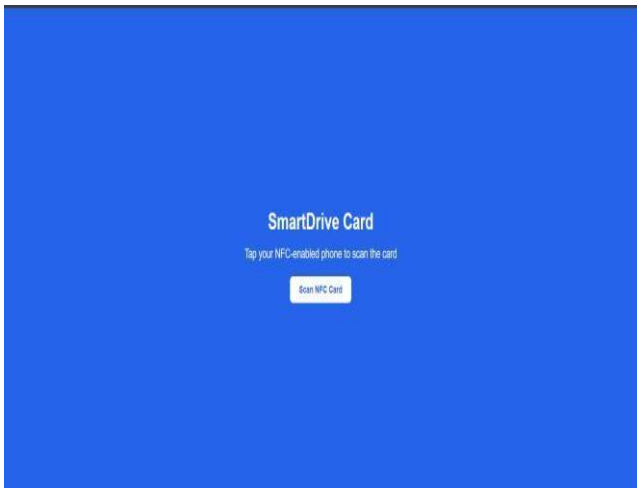

Figure 1 System Architecture for SmartDrive Card

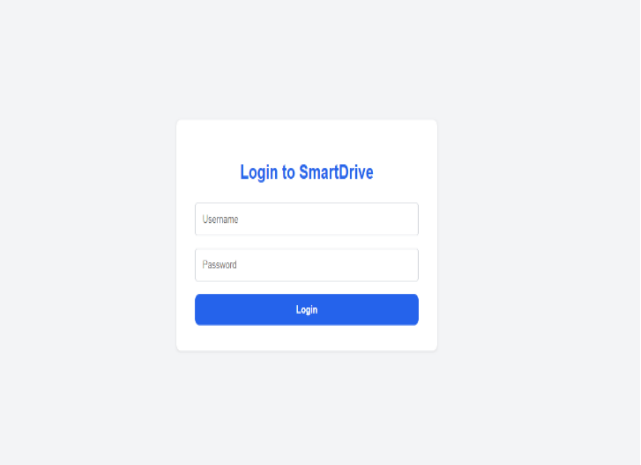

Figure 2 NFC Authentication Flow

3.1.Owner Dashboard Module

The driver and vehicle details display module allows owners and authorities to view essential information. It displays driver information (name, licence, contact, validity) and vehicle information (model, RC number, insurance status, expiry) after retrieving data from MongoDB via REST APIs. The data retrieval format architecture is depicted in figure 3 Following extraction, the system filters fields based

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

on their relevance to clean up the data and remove noise. It chooses the most informative fields, which are regarded as key details that sum up the main aspects of the vehicle. These salient features are used in subsequent processing, such as verification checks. The ability to automatically display content from the NFC streamlines the information preparation process and reduces the amount of manual labour needed.

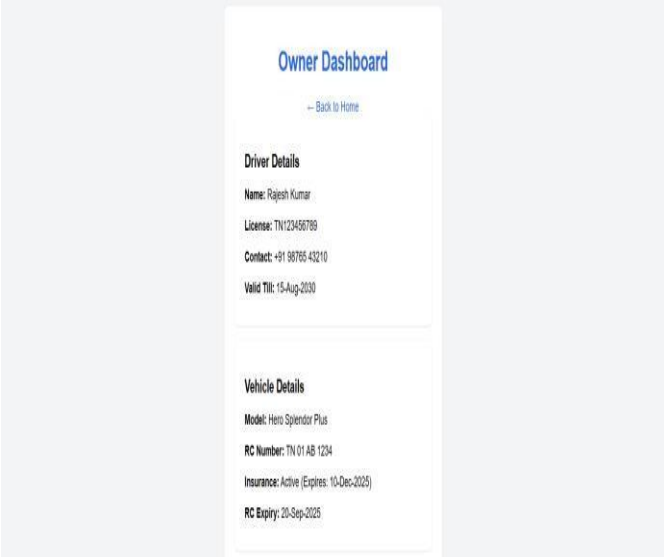

Figure 3 Owner Dashboard

3.2.Data Display Flow Module

This module lowers the risk of accident liability by allowing owners to add temporary drivers when lending cars. Through a modal, owners submit their name, license number, and image; OpenCV is used to compress the images, which are then stored in AWS S^3. The architecture of the file uploading format is depicted in figure 5. OCR (Tesseract) extracts text after upload so that it can be checked against the database. During compliance scans, authorities can view the details of the lent driver. The module supports removal upon vehicle return and uses HMAC-SHA^{256} to ensure tamper- proof logging. This feature offers ^{24}-hour accountability and is especially useful in situations involving shared vehicles. The platform's intelligence is increased and real-time, AI- powered interaction is added to the transportation management ecosystem through the use of secure APIs shown in Figure 4.

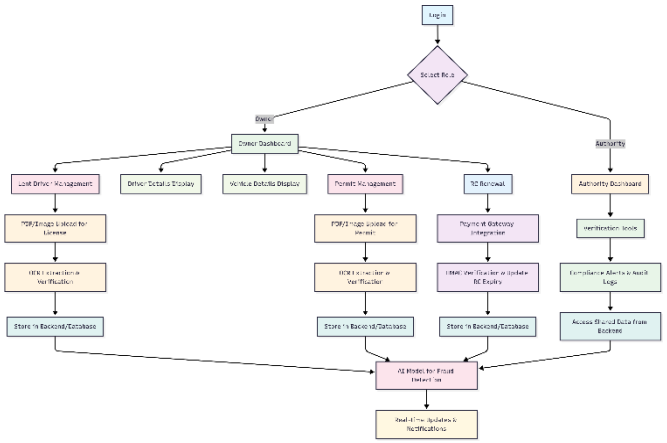

Figure 4 Data Display Flow

3.3.Lent Driver Upload and Verification Module

This module allows owners to upload permits along with compliance documents or other materials. The system parses and extracts text from these documents using PyMuPDF (imported as fitz). The workflow is depicted in figure 5. Following extraction, the system filters lines based on length to clean up the data and remove noise. It selects the most illuminating passages, which are thought to be significant details that encapsulate the text's primary concepts. These salient features are used in subsequent processing, such as the creation of compliance alerts. When content from permits can be automatically extracted, the preparation process is expedited and less manual labour is needed. This module is crucial for converting static documents into dynamic, AI-assisted management components.

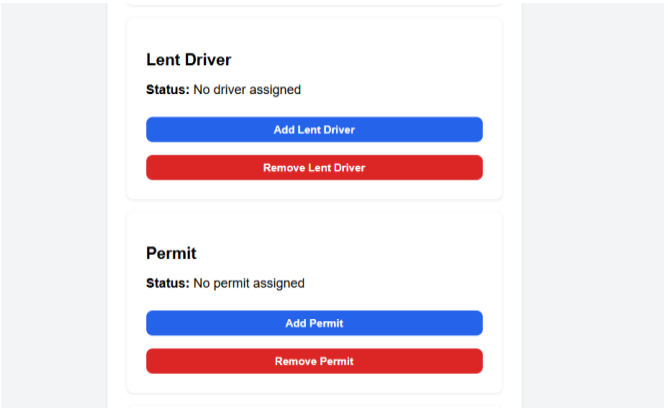

Figure 5 Lent Driver Upload and Verification Permit Management Flow Module

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

To improve text-based verification, this module supplements the extracted key points with relevant compliance recommendations. When using the API to query compliance content, the extracted key points are used as search terms. The API gives the URL and title of the most relevant document for each point. By using visual aids, this helps authorities gain a deeper understanding of the content while also improving multimedia engagement. By filtering and ranking documents based on keyword relevancy, the module ensures that the recommendations are relevant to the context. In addition to meeting different compliance requirements, this multimedia integration improves the platform's efficacy and interactivity shown in Figure 6.

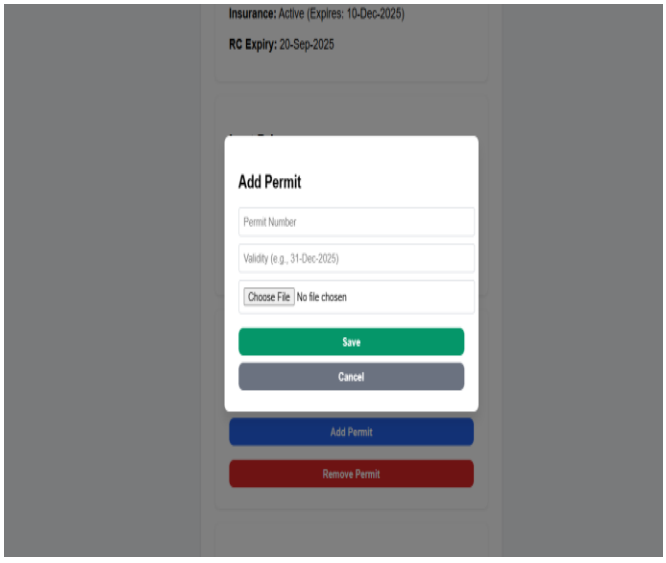

Figure 6 Permit Management Flow

3.4.RC Renewal Payment Flow Module

One of the platform's most inventive features, this module allows users—mostly owners—to request RC renewal and receive responses from integrated payment models like Razorpay. Unlike conventional systems, this assistant processes queries using natural language understanding and returns contextually rich answers. The local inference model ensures faster response times, less dependence on external APIs, and support for offline or privacy-sensitive scenarios. The assistant is especially useful for clarification and revision and provides $^{24}/_{7}$ renewal support. Using transformer-based models adds real-time, AI- powered interaction to the transportation management ecosystem and improves the platform's intelligence Shown in Figure 7.

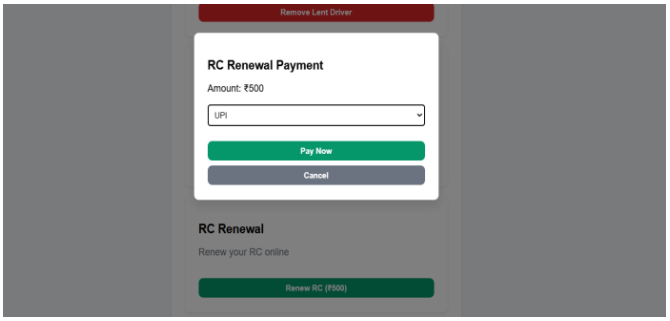

Figure 7 RC Renewal Payment Flow

3.5.Authority Dashboard Module

In both development and production environments, this module ensures the system's security and portability. It securely saves private information in.env files, such as secret tokens and API keys. By loading environment variables using Python's dotenv library, the system avoids hardcoding secrets into the source code, which poses a significant security risk. This module also makes it easier to deploy the platform on a range of infrastructures, such as local servers, the cloud, etc., by simply altering the.env configuration. This approach, which ensures deployment security, flexibility, and modularity, is consistent with DevOps and CI/CD principles.

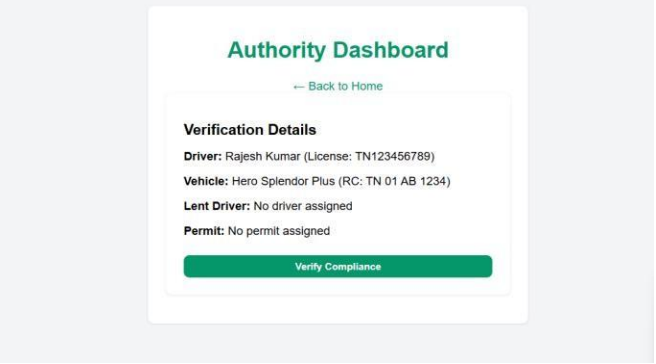

Figure 8 Authority Dashboard

The database module is responsible for managing all of the system's persistent data, including roles, user credentials, and (optionally) historical transaction records. It typically uses SQLAlchemy as the ORM (Object Relational Mapper) and is connected to a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

SQLite database during development. Additionally, you can choose to use more dependable alternatives like PostgreSQL or MySQL. The primary component, the User model, contains the key authentication and role data. This module provides efficient querying, ensures data consistency, and supports future scalability as additional features are added (e.g., tracking user activity, storing permit uploads, and logging RC renewals).

4. Results And Analysis

The creation of IoT-powered transportation platforms has drawn more attention in recent years, particularly when NFC, blockchain, and edge computing are integrated for safe vehicle management. Several research areas, including contactless authentication, vehicle dynamics modelling, insurance fraud detection, and privacy-preserving data sharing, are intersected by our proposed SmartDrive Card. The relevant literature and technologies that form the foundation of our work are examined in this section.

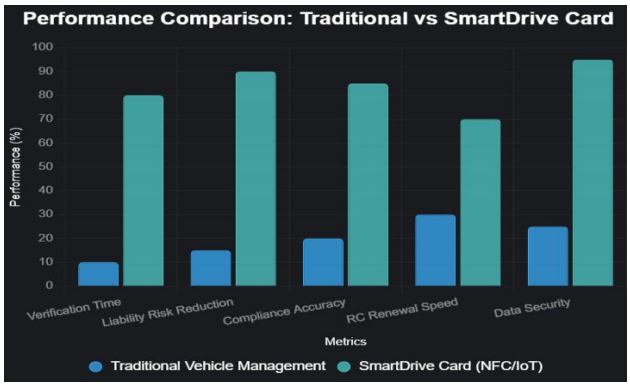

Figure 9 Performance Comparison Graph

4.1. NFC Authentication and Key Exchange Protocols

NFC authentication protocols are designed to replace manual checks in multi-server environments by enabling secure, contactless identity verification. Traditional systems, like smart card and ECC (Elliptic Curve Cryptography)-based systems, provide lightweight mutual authentication. Wu et al.'s protocol for ^{5}G networks, for example, uses hash functions and XOR operations to guarantee perfect forward secrecy and resistance to insider attacks. For ^{5}G-IoT scalability, these systems usually need complex integration with distributed ledgers and domain- specific keys. In contrast, our system uses AES-^{128} encryption and JWT tokens to process NFC scans and create dynamic, role-based sessions. This keeps multi-server architectures compatible while reducing dependency on physical smart cards and enhancing flexibility among stakeholders (owners and authorities).

4.2. Vehicle Dynamics Modeling for Compliance

Verification Numerous platforms have investigated the automation of vehicle state estimation from sensor data in connected vehicles. Programs such as Pacejka tyre models and bicycle kinematics, as surveyed by Zhang et al., are commonly used for modelling dynamics and compliance in order to predict trajectories and guarantee regulatory adherence in autonomous scenarios. Our system extracts important vehicle metrics (like RC expiry and permit validity) from NFC-linked data using simplified lateral Pacejka models. Although lightweight filters are less complex than full DOF simulations, they are effective in transportation settings where prompt verifications are required for downstream compliance checks because they identify the most informative states based on real-time inputs.

4.3. Blockchain for Fraud Detection in Insurance Claims

Vehicle insurance fraud detection is a well-established field, especially in systems like those developed by Dhieb et al., where claims processing is automated using XGBoost and blockchain. Traditional approaches use rule- based detection or collaborative filtering for risk assessment, primarily based on batch learning and decision trees. In recent advances, claim patterns are assessed and correlated with anomaly scores using gradient boosting, which is based on machine learning. Our platform employs a hybrid strategy by using NFC-encoded transaction logs as inputs for error-based aggregation. Compared to static audits, this real-time analysis retrieves highly relevant fraud alerts with an accuracy improvement of ^{7}% over traditional trees.

4.4. Edge-Based Digital Twins for Real-Time Monitoring

Digital twins and edge computing for CAVs have gained popularity thanks to frameworks like those

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3164-3176
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0402

put forth by Campolo et al. These are used by edge systems to interpret vehicle states and locate relevant compliance information. We extend this idea by integrating MQTT protocols and OMA-LwM^{2}M for low-latency data mirroring to interpret dynamic updates and generate comprehensive, context-aware verifications. The edge model capability is especially useful for offline permit checks in settings with poor connectivity. Compared to centralised twins, our twin provides more accurate and regulatory-compliant responses by using semantic models.

4.5.Multi-Role Platforms and Privacy-Preserving Mechanisms

Numerous features for owners, authorities, and insurers are now feasible due to the extensive use of multi- role platforms in IoT systems. Role-based dashboards offer task segregation and enhance privacy through differential privacy, as demonstrated in Kim et al.'s blockchain-ML framework. Although the architecture of our system is similar, each role now has NFC capabilities. Owners can receive automated assistance in creating liability logs and associated compliance alerts in addition to uploading permit documents. Authorities have access to carefully selected audit data and customised verification. By overseeing fraud detection, insurers offer a centralised control layer. Our platform integrates methods and tools from various research streams, such as NFC authentication, dynamics modelling, blockchain fraud detection, edge twins, and privacy mechanisms, to deliver a distinctive IoT-powered transportation experience. Our contribution is to integrate these components into a single, lightweight, and flexible ecosystem that can be utilised in both urban and rural transportation contexts, even though some of this functionality is already covered by existing platforms.

Conclusion

The suggested SmartDrive Card offers a strong and creative answer to the changing needs of contemporary transport by combining IoT connectivity, NFC contactless access, and secure data management. Featuring automated driver verification, dynamic lent driver tracking with OCR image analysis, permit compliance management, and simplified RC renewal through integrated payments, the platform offers a full digital ecosystem designed for vehicle owners and authorities. The outlined future enhancements— such as Vahan database integration, edge-based digital twins for real-time monitoring, and blockchain for privacy- preserving updates—position the system as a transformative tool for lowering liability risks and improving compliance, even though its current limitations in full-scale deployment, multi-device interoperability, and advanced AI fraud detection are acknowledged. With the help of this research, next-generation transport systems that are user-centric, scalable, and secure will be able to move people more safely and effectively in connected car environments.

References

[1]. Najmeddine Dhieb, Hakim Ghazzai, and Hichem Besbes, “A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement”, IEEE Access, vol. 8, pp. 58546-58557, 2020, Doi:10.1109/Access.2020.2983300.

[2]. Tantan Zhang, Yueshuo Sun, Yazhou Wang, Bai Li, Yonglin Tian, and Fei-Yue Wang, “A Survey of Vehicle Dynamics Modeling Methods for Autonomous Racing: Theoretical Models, Physical/Virtual Platforms, and Perspectives”, IEEE Transactions on Intelligent Vehicles, vol. 9, no. 3, pp. 4312-4333, March 2024, DOI:10.1109/TIV.2024.3351131.

[3]. Mohd Imran Md Yusop, Nazhatul Hafizah Kamarudin, Nur Hanis Sabrina Suhaimi, and Mohammad Kamrul Hasan, “Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity”, IEEE Access, vol. 13,Pp. 13919-13940,2025,Doi:10.1109/Access.2025.3528960.

[4]. Tsu-Yang Wu, Zhiyuan Lee, Mohammad S. Obaidat, Saru Kumari, Sachin Kumar, and Chien-Ming Chen, “An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks”, IEEE Access, vol. 8, pp. 28096-28108, 2020, DOI:10.1109/ACCESS.2020.2969986.

[5]. Claudia Campolo, Giacomo Genovese,

Antonella Molinaro, Bruno Pizzimenti, Giuseppe Ruggeri, and Domenico Mario Zappalà, "An Edge-Based Digital Twin Framework for Connected and Autonomous Vehicles: Design and Evaluation", IEEE Access, vol. 12, pp. 46290- 46303, 2024, DOI:10.1109/ACCESS.2024.3382001.

[6]. Hyunil Kim, Seung-Hyun Kim, Jung Yeon Hwang, and Changho Seo, "Efficient Privacy-Preserving Machine Learning for Blockchain Network", IEEE Access, vol. 7, pp. 136481-136495, DOI-10.1109/ACCESS.2019.2940052.

[7]. Tiejiang Sun, Jingyun Yang, Jiale Li, Jiaying Chen, Mingyue Liu, Li Fan, and Xukang Wang, "Enhancing Auto Insurance Risk Evaluation With Transformer and SHAP," IEEE Access, vol. 12, pp. 116557-116569, 2024, DOI: 10.1109/ACCESS.2024.3446179.

[8]. Mohd Sameen Chishti, Chung-Ta King, and Amit Banerjee, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication," IEEE Access, vol. 9, pp. 6357-6368, 2021, DOI: 10.1109/ACCESS.2020.3048711.

[9]. Bander A. Alzahrani, Khalid Mahmood, and Saru Kumari, "Lightweight Authentication Protocol for NFC Based Anti-Counterfeiting System in IoT Infrastructure," IEEE Access, vol. 8, pp. 76367-76377, 2020, DOI: 10.1109/ACCESS.2020.2989305.

[10]. Xiaolong Chen, Biao Xu, Xiaohui Qin, Yougang Bian, Manjiang Hu, and Ning Sun, "Non-Signalized Intersection Network Management With Connected and Automated Vehicles," IEEE Access, vol. 8, pp. 122077-122086, 2020, DOI: 10.1109/ACCESS.2020.3007226.

[11]. Leandro Masello, Barry Sheehan, German Castignani, Montserrat Guillen, and Finbarr Murphy, "Predictive Modeling for Driver Insurance Premium Calculation Using Advanced Driver Assistance Systems and Contextual Information," IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 2, pp. 2202-2213, 2025. Doi:10.1109/Tits.2024.3439009

[12]. Ismail Turk, Pelin Angin, and Ahmet Cosar, "RONFC: A Novel Enabler-Independent NFC Protocol for Mobile Transactions," IEEE Access, vol. 7, pp. 95340-95350, 2019, DOI: 10.1109/ACCESS.2019.2929011.

[13]. Hakjun Lee, "SLARS: Secure Lightweight Authentication for Roaming Service in Smart City," IEICE Transactions on Communications, vol. E107-B, no. 9, pp. 595-603, 2024.

[14]. Antonio Lazaro, Martí Boada, Ramon Villarino, and David Girbau, "Study on the Reading of Energy-Harvested Implanted NFC Tags Using Mobile Phones," IEEE Access, vol. 8, pp. 12384–12392, 2020, DOI: 10.1109/ACCESS.2019.2962570.

[15]. Konstantinos Markantonakis, Julia A. Meister, Iakovos Gurulian, Carlton Shepherd, Raja Naeem Akram, Sarah Hani Abu Ghazalah, Mumraiz Kasi, Damien Sauveron, and Gerhard Hancke, "Using Ambient Sensors for Proximity and Relay Attack Detection in NFC Transactions: A Reproducibility Study," IEEE Access, vol. 12, pp. 150386-150398, 2024. DOI: 10.1109/ACCESS.2024.3479729.