Journal of Robotics and Control (JRC)
Volume 6, Issue 5, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i5.26057

Robotics-Driven Biometric Authentication for Secure and Intelligent Vehicle Access

Vishnu G. Nair [1], Madala Chaitanya Sai [2], Spoorthi Singh [3*], Navya Thirumaleswar Hegde [4*], Manish Varun Yadav [5]
[1, 2, 4, 5] Department of Aeronautical and Automobile Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education Manipal Udupi, Karnataka, India
[3] Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education Manipal Udupi, Karnataka, India
Email: [1] vishnu.nair@manipal.edu, [2] madala.sai@learner.manipal.edu, [3] spoorthi.shekar@manipal.edu, [4] navya.hegde@manipal.edu, [5] yadav.manish@manipal.edu
*Corresponding Author

***Abstract*—As modern vehicles increasingly adopt intelligent systems, the need for robust and secure access control mechanisms has become paramount. This study presents a dual modal biometric authentication framework integrating fingerprint and iris recognition to enhance vehicular security and user convenience. The system leverages strategically positioned sensors—capacitive fingerprint scanners embedded within door handles and high-resolution iris scanners mounted near the driver's entry point—coupled with a central microcontroller for real-time processing. Lightweight image processing and matching algorithms are implemented to ensure fast and accurate authentication under varied environmental conditions. The proposed system was validated on a prototype vehicle model using biometric data from over 50 users, demonstrating high accuracy, low false acceptance/rejection rates, and resilience to spoofing attacks. In addition to technical implementation, the study addresses practical challenges including sensor placement, processing constraints, data privacy, and system usability. The findings support the feasibility of integrating multimodal biometric authentication in vehicles, offering a secure, user-friendly alternative to conventional key- based systems. This research is supported by Indian patent file number 202441019532.**

Keywords—Biometric Authentication; Artificial Intelligence; Cyber-Physical Security; Robotics Integration; Vehicle Access Control; Data Privacy.

I. INTRODUCTION

Vehicle security systems play a critical role in mitigating unauthorized access, preventing theft, and ensuring the safety of vehicle occupants. These systems typically incorporate a central processing unit integrated with multiple sensors distributed throughout the vehicle to detect security-related events such as unauthorized entry, forced ignition attempts, and anomalous vehicle movements. Commonly used sensors include motion detectors, door and window position sensors, and vibration sensors. The controller continuously processes signals from these sensors and, upon detecting suspicious activity, triggers an alert mechanism, often involving flashing lights and an audible alarm through the vehicle horn [1], [2].

The rapid advancement of intelligent transportation systems has ushered in an era of connected and autonomous vehicles, offering unprecedented levels of convenience, automation, and user interaction. However, this growing complexity has also made modern vehicles increasingly vulnerable to security breaches. Traditional access methods such as mechanical keys and wireless key fobs, once considered secure, are now frequently exploited through relay attacks, key cloning, and electronic signal manipulation. These vulnerabilities highlight a pressing need for more secure, context-aware, and user specific vehicle authentication systems. Biometric authentication technologies—such as fingerprint recognition, iris scanning, facial recognition, and voice identification—have emerged as promising alternatives to conventional key-based access. These systems offer the advantage of using physiological and behavioral traits that are unique, difficult to replicate, and non-transferable. Yet, despite their potential, the application of biometrics in automotive contexts remains limited due to several practical and technical challenges. These include inconsistent performance under variable environmental conditions (e.g., lighting, temperature, and user movement), susceptibility to spoofing, and a lack of redundancy in unimodal systems. Prior studies have explored individual modalities in isolation, but few have addressed these challenges through integrated, real-world deployable frameworks. This study aims to bridge that gap by proposing a dual-modal biometric authentication system for vehicle access, combining fingerprint and iris recognition technologies to improve robustness and accuracy. The system is designed to function under real-world constraints and is supported by robotics-driven sensor integration and AI-based processing for real-time decision-making. This approach not only enhances security but also improves user convenience through seamless, intuitive interactions. By critically evaluating the shortcomings of existing systems and integrating interdisciplinary technologies from robotics, artificial intelligence, and cybersecurity, this work contributes to the development of a next-generation vehicular security framework. The proposed solution is positioned as a scalable and practical alternative to traditional and single-modality biometric systems, aligning with the growing demand for secure and intelligent transportation solutions.

With the rise of sophisticated automotive cyber-attacks and evolving theft techniques, traditional security measures are increasingly vulnerable. Wireless key entry systems, once considered a secure alternative, are now susceptible to relay attacks, where adversaries intercept and replicate key signals to gain unauthorized access [3], [4]. To enhance vehicular

CC BY SA

security, there is a growing interest in integrating biometric authentication, leveraging robotics and artificial intelligence to enable secure and seamless access control [2]. Biometric authentication utilizes unique physiological or behavioral traits, such as fingerprint recognition, facial analysis, and voice identification, offering a robust alternative to conventional key- based systems. However, challenges persist in ensuring the reliability, privacy, and cost-effectiveness of biometric security frameworks in real-world automotive applications. For broad adoption, such systems must be designed to operate effectively under diverse environmental conditions while maintaining computational efficiency. Moreover, compliance with regulatory standards and ethical considerations is essential in deploying biometric authentication within intelligent vehicle ecosystems. This paper explores the feasibility of robotics-driven biometric security in modern automobiles, examining sensor integration, machine learning-based authentication, and the implications for automotive cybersecurity.

In the rapidly evolving domain of automotive technology, integrating advanced innovations is pivotal in enhancing both security and convenience for vehicle owners. Among these advancements, biometric authentication systems have emerged as a promising alternative to traditional key-based entry methods. Biometric security leverages unique physiological traits to provide a seamless and secure authentication mechanism, with fingerprint sensors and iris scanners being two prominent options. Fingerprint recognition, a widely adopted biometric authentication technology, offers a swift, secure, and user-centric approach to vehicle access. By analyzing the unique ridge patterns on an individual's fingertips, this technology enables users to unlock doors, start engines, and access personalized vehicle settings without the need for physical keys or electronic fobs. The integration of fingerprint sensors in automotive systems has the potential to revolutionize vehicle security by mitigating key theft and unauthorized access. However, practical challenges must be considered when implementing biometric authentication in real-world scenarios. Factors such as gloved hands, dirt, or injuries may temporarily hinder fingerprint recognition, necessitating an alternative authentication method to ensure consistent and reliable vehicle access. In such situations, an iris scanner serves as an effective fallback option, leveraging the unique patterns in the user's iris for secure authentication. Iris recognition is particularly advantageous due to its high accuracy and resistance to external environmental factors, making it a viable secondary authentication mechanism in automotive applications. The adoption of biometric authentication in vehicles necessitates a multidisciplinary approach, incorporating robotics, artificial intelligence, and embedded systems to optimize sensor integration, data processing, and real-time authentication. Additionally, considerations regarding cybersecurity, data privacy, and regulatory compliance must be addressed to facilitate the widespread implementation of biometric-based vehicle security systems.

Iris identification technology leverages the intricate and highly unique patterns found in the human iris, which remain stable over time, making it a robust biometric authentication method [5]–[7]. When fingerprint authentication becomes im- practical due to factors such as gloved hands, dirt, or injuries, an iris scanner serves as a complementary access method. This dual biometric approach ensures continuous and secure vehicle access while maintaining a seamless and user-friendly experience, aligning with the increasing demands for advanced auto- motive security. This study explores the integration of biometric authentication in automotive systems, focusing on the synergy between iris scanners and fingerprint sensors. By combining these modalities, we address practical challenges associated with single-method authentication, offering an adaptable and resilient solution for vehicle access. The technical capabilities, security advantages, usability, and potential limitations of these technologies are examined, highlighting their role in shaping a sophisticated, secure, and user-centric future for vehicular authentication. The implementation of both biometric systems allows users to seamlessly transition between authentication methods based on environmental and physical conditions. For instance, while a capacitive fingerprint sensor serves as the primary means of access, an iris scanner provides an alternative for scenarios involving gloves or obstructed fingerprints. A capacitive fingerprint sensor consists of a readout circuit connected to multiple sensor components, with dielectric material covering the sensor cells where fingers are placed [8], [9]. Each component includes an active sensing cell that detects variations in the electric field caused by the proximity of fingerprint ridges to the sensor plates. The circuit arrangement for the operation of a capacitive fingerprint sensor is illustrated in Fig. 1. The capacitive fingerprint sensor functions by detecting variations in input voltages when in contact with a fingerprint. A controller oversees these voltage fluctuations in the sensing process, converting them into data or images through an image processing unit. During initial registration, the processed fingerprint gets stored in a database. The feature extraction and template generation unit identify and isolates distinct features from the processed data or images. Subsequently, during authentication, the matching unit compares the extracted features from the user's fingerprint with the stored templates in the database. Access is granted if a match is found; otherwise, additional authentication steps may be necessary. By measuring the capacitance values resulting from ridges and valleys, an electronic representation of the fingerprint pattern is generated. While capacitive sensors may struggle to read fingerprints when hands are soiled or sweaty, their ability to withstand rugged conditions makes them suitable for automotive use. Strategic placement of sensors can further enhance their shielding from environmental conditions and improve accuracy without significantly impacting cost [8], [9]. Iris scanning has emerged as a viable alternative for biometric access, primarily due to its reliability and ease of authentication. A high-resolution camera captures a simple picture of the iris, which is then mapped and stored as a reference for subsequent access requests. This stored image is processed to generate a unique pattern used for authentication [6], [10]. Conventional key fob systems for vehicle unlocking pose significant security risks, as advancements in technology enable burglars to exploit vulnerabilities and gain unauthorized access without triggering alarms [2]. Mechanical keys, once relied upon for

physical security, are prone to manipulation techniques like lock picking and bumping, necessitating the adoption of electronic keys with enhanced features [11].

This paper presents a novel dual-modal biometric authentication system for vehicular security that integrates capacitive fingerprint scanning and iris recognition to enhance access control robustness and user convenience. The study advances the state- of-the-art by proposing strategic ergonomic sensor placement within vehicle architecture—embedding the fingerprint sensor in the inner door handle and the iris scanner in the B-pillar—to ensure seamless, intuitive user interaction. Additionally, the methodology introduces a multi-tiered authentication logic that balances security with usability by adapting to authentication failures through progressive escalation. Supported by an Indian patent filing, this work lays foundational groundwork for secure, AI-enabled vehicle access systems, addressing key challenges in environmental adaptability, data privacy, and system integration. The research contributes to the broader field of intelligent transportation systems by offering a practical and scalable framework for next-generation vehicular biometric security solutions.

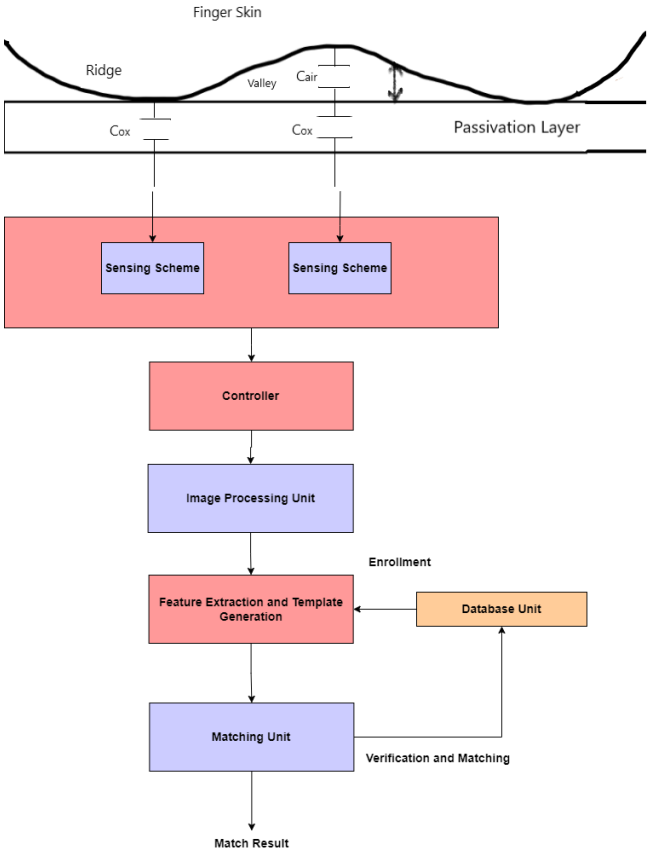

Fig. 1. Capacitive sensor circuitry for fingerprint recognition, uses ridges and valleys for creating an electrical pattern for the fingerprint [8]

II. EASE OF USE

Recent advancements in Internet of Things (IoT), Programmable Logic Controller (PLC), and communication technologies have made Autonomous Vehicles (AV) a reality, with model vehicles already traveling thousands of miles in test driving. Moving forward, the development of Autonomous Intelligent Vehicles (AIV) is necessary to make effective decisions on road networks, addressing technical and non-technical challenges such as software complexity and real-time data analysis [12]. Vehicle security is critically important, especially as thefts often occur in parking lots and other unsecured areas. Originally, vehicles were secured with mechanical keys, which are susceptible to lock picking and bumping, compromising their reliability in protecting vehicles [2]. This vulnerability led to the development of electronic key systems, introducing new features to both the locking and starting mechanisms of vehicles [11]. However, these electronic key fobs, which transmit an encrypted code wirelessly to unlock the vehicle, also pose security risks. Advances in technology now allow thieves to intercept, decrypt, and replicate the key fob's signal from a distance, enabling them to unlock cars without setting off alarms.

Biometric systems provide a robust solution for secure authentication by utilizing unique human traits such as fingerprints, iris patterns, and facial features. Unlike traditional methods which rely on passwords and PINs, biometric authentication offers the convenience of accessing systems without the need to remember complex codes [12]. These systems automatically recognize individuals based on their biological and behavioral characteristics, enhancing both security and user convenience [13]. Biometric methods leverage unique physical and psychological traits that distinguish individuals, ensuring that biometric data is inherently non-transferable and non- shareable [14]. Among various biometric techniques, iris recognition is particularly noted for its accuracy. This method is non- invasive due to the overt nature of the iris, which is crucial for user acceptance in practical applications [15]. Iris recognition involves several critical processes: capturing the image (Image Acquisition), preparing the image for analysis through seg- mentation and normalization (Image Pre-Processing), extracting relevant features (Feature Extraction), and finally, matching these features against a pre-existing database to verify identity (Iris Recognition System) [16]. This sequence of steps ensures a high level of precision in authenticating identities based on iris patterns.

Fingerprint-based identification has gained significant traction as a key biometric technology due to its unique reliability and foolproof nature, as fingerprints are unique to each individual. This technology bifurcates into two main categories: fingerprint verification and identification. Fingerprint verification processes involve confirming or denying an individual's claimed identity through a one-to-one matching of their fingerprint. Conversely, fingerprint identification involves a many- to-one match, determining the specific registered user that a particular fingerprint belongs to [17]. Recognized for its efficiency, security, cost-effectiveness, and user-friendly interface, fingerprint biometrics not only serves traditional applications like intellectual property protection and commercial profits but is also increasingly utilized in the automotive industry to bolster security measures and prevent vehicle theft [18].

The use of single-modality biometric systems has been prevalent for both verification and identification purposes. However, as these systems are increasingly deployed in sectors like automotive security, they encounter challenges including the need for extensive population coverage,

accommodation of demographic diversity, varied deployment environments, and elevated performance expectations. These challenges often exceed the capabilities of single-modality systems, necessitating an integrated approach that leverages additional sources of biometric data [19]. In automotive security, adopting a multi- biometric system that combines various biometric traits, algorithms, sensors, and other components can significantly enhance the accuracy and reliability of recognition decisions. Such systems not only improve accuracy but also extend population coverage, offer robustness against spoofing, and reduce enrollment failures [20]. Iris recognition, for instance, exemplifies a highly reliable biometric technique. It utilizes the unique patterns in an individual's iris, which are stable and distinctive, making it highly effective for accurate identification. This method surpasses traditional security mechanisms like magnetic stripe cards and passwords, which depend solely on retrievable stored data, by utilizing inherent individual characteristics [21]. Multi- modal biometrics integrate various technologies, including iris, face, fingerprint, hand geometry, and voice recognition. Each technology possesses unique advantages and shares critical attributes such as universality, uniqueness, permanence, collectability, performance, and acceptability. These attributes vary in their degree of importance depending on the specific application context [22]. In the context of vehicular security, multi- modal biometrics enhance access control systems, significantly mitigating the risks of unauthorized access and vehicle theft. This integrated approach is crucial for ensuring the security and integrity of vehicles in today's technologically advanced environment.

In the realm of fifth-generation (5G) mobile networks, Multi- access Edge Computing (MEC) offers reduced latency and network strain by processing data closer to the user. To enhance user privacy in this context, we propose a Privacy-Aware Access Control (PAAC)-based Biometric Authentication Protocol (BAP) that employs fuzzy extractor techniques for secure, efficient, and real-time biometric data access at the network edge [23]. The Smart Grid (SG) has led to the development of several authentication and key agreement frameworks designed to secure data transmission and preserve user privacy. To address the limitations of existing frameworks, we intro- duce a Security Enhanced Lightweight Authentication and Key Agreement Framework (SE-LAKAF) that uses fuzzy extractors, elliptic curve cryptography, and AES-based hybrid encryption, ensuring robust security against various network attacks and maintaining user anonymity with competitive overheads [24]. In [25], the authors introduce a secure authentication scheme for Vehicle Fog Service (VFS) that employs blockchain and physical unclonable function (PUF) technologies to enable two-way authentication among on-board units (OBU), road side units (RSU), and untrusted fog nodes, while ensuring conditional anonymity and non-repudiation. Our scheme enhances security by avoiding extensive certificate revocation list checks, thereby reducing computational overhead, and it has been formally and informally validated as secure against a variety of attacks, making it a cost-effective solution for secure VFS environments. An informative survey paper is given in [26], which delves deeply into fog computing, examining its architecture, features, and security aspects, alongside a thorough analysis of existing authentication mechanisms, their functionality, performance, and limitations. The authors also offer a taxonomy of security issues within fog computing, aiming to guide future research and address the challenges in designing robust authentication systems for secure communication in this increasingly vital technology domain. The research in [27] aims to bolster transportation security systems by implementing a deep learning-based multimodal biometric authentication network (MMBA-Net), which utilizes multilayer convolutional neural networks (ML-CNN) for feature extraction and Deep Hashing Component Analysis (DHCA) for feature compression Experimental results on large-scale datasets validate the effectiveness of DHCA in enhancing the reliability and efficiency of biometric authentication in transportation security systems. The study in [28] underscores the significance of addressing fingerprint alteration and obfuscation, which poses a significant challenge to security and investigative agencies. By highlighting various techniques used for fingerprint obfuscation, forgery, and alteration, it emphasizes the importance of identifying and interpreting these alterations and recommends informing law enforcement agencies to mitigate potential threats. To address the increasing incidence of vehicle theft worldwide, [29] proposed a decentralized and secure framework utilizing blockchain and smart contracts for enhanced vehicle security. The framework incorporates 2-Step Authentication (2SA) and unauthorized access detection algorithms to ensure secure access to the vehicle application while preserving owner privacy and enabling multiple authorized drivers.

The paper [30], introduces a Blockchain-based Vehicle Anti- Theft System (BVATS) utilizing smart contracts to address issues such as data leakage, centralized systems, and key management in existing vehicle anti-theft systems. BVATS leverages blockchain's decentralized architecture and smart contract technology to provide a secure, immutable platform for vehicle security, allowing multiple authorized drivers while maintaining data integrity. The study in [31] introduces a novel vehicular ad hoc network (VANET) routing protocol using genetic algorithm (GA) and evolution-based techniques to optimize route selection, while also proposing a cryptography- based mechanism for securing V2V and V2I communications. By integrating AOMDV-RGA for route selection and ABSC for secured communication, the proposed hybrid approach demonstrates enhanced performance in addressing routing and security challenges in VANETs compared to existing techniques. The article [32] introduces a secure and robust authentication protocol for fog-based vehicular communication, addressing vulnerabilities present in conventional approaches while minimizing latency, computation, communication, and storage costs. Formal security verification and performance comparison demonstrate the protocol's effectiveness against threats and its suitability for practical application. In [33] the authors present BLOcKeR, a novel access control scheme that integrates biometrics with physically unclonable functions (PUFs) and hardware obfuscation to protect against physical attacks and unauthorized access in IoT systems. BLOcKeR ensures system activation without storing raw biometric data, providing irreversibility, unlikability, and

revocability to templates, and has been extensively evaluated for security against over 45,000 attack variants. Another informative review [34] explores the applications of biometric technology in educational institutions, highlighting its role in identity management, attendance tracking, e-evaluation, and other areas. Despite the promising growth outlook for biometric technology, addressing security and privacy concerns remains a critical challenge for its widespread adoption in education. In [35], the authors introduce a lightweight bio- cryptosystem designed for securing biometric templates in IoT applications, addressing constraints in power and memory space. The proposed architecture employs a three-stage process involving key generation, confusion, and diffusion, utilizing a novel DNA encoding method to reduce computational complexity and enhance security. The study provided in [36] aims to devise, implement, and evaluate a dynamic authentication scheme for geospatially enabled vehicular networks leveraging blockchain technology to enhance safety and transportation efficiency. Demonstrated security, correctness, and suitability for vehicular systems are established through rigorous analysis, including formal verification with the random oracle model and informal security analysis using the AVISPA tool. In [37], the authors introduced a novel privacy-based authentication algorithm for enhancing data transmission accuracy in smart VANET transportation. By employing a lightweight hybrid authentication-based privacy-preserving approach and an efficient congestion-based clustering algorithm, the proposed method achieves significant improvements in throughput, QoS, latency, computational cost, and data transmission rate, demonstrating resilience against various security and privacy threats.

The review in [38] explores the intersection of artificial intelligence (AI) and transportation security, focusing on electric and aerial vehicles (EnAVs). By analyzing the evolving threat landscape and the vulnerabilities of advanced vehicles, it highlights AI's potential in addressing security challenges, covering areas such as vehicle surveillance, cybersecurity, decision-making, and control through reinforcement learning. The research in [39] introduced a novel approach to anonymous identity authentication in vehicular networks using batch verification techniques, bolstering privacy in IEEE WAVE's security services. By employing zero-knowledge proofs and batch verification, the proposed method enhances privacy in applications such as near-field vehicle payment and DSRC security services, with experimental results indicating lower computational overhead compared to competing systems for signature batches up to eleven. In [40], the authors explore the advancements and challenges in deep multimodal learning within the computer vision domain, offering insights into key concepts and algorithms for integrating heterogeneous visual cues across sensory modalities. It summarizes perspectives such as multimodal data representation, fusion techniques, multitask learning, alignment, transfer learning, and zero-shot learning, along with discussing current applications and benchmark datasets, while also outlining future research directions and addressing existing limitations and challenges.

The work presented in [41] delves into the implications of somatic surveillance, which relies on behavioral biometrics and sensory algorithms for unobtrusive data gathering. It examines the need for a legal framework to address the shifting dynamics of human-machine interactions and proposes a reevaluation of legal accountability, considering the role of autonomous sensing agents in cyber-physical spaces. The study in [42] examines the intersection of digital technologies and privacy concerns in the marketing landscape, proposing a conceptual framework that delineates firm and consumer responses to privacy tensions. Through a synthesis of perspectives and empirical insights, the authors present a typology of firms based on their data strategies, offering insights into how different approaches impact firm performance within the context of evolving privacy concerns.

In [43], the authors explore the implementation of a Multi- Objective Optimization technique to enhance public transportation route planning in smart cities, considering factors like traffic patterns, cost, and environmental impact. By utilizing real-world data and complex algorithms, the research demonstrates the effectiveness of the proposed approach in improving time efficiency, reducing costs, and minimizing environmental footprints, offering valuable insights for the advancement of smart city transportation systems. The paper in [44] highlights the fragmented nature of European legal norms concerning facial recognition technology in law enforcement, which may impede its lawful use. It advocates for the development of a dedicated law based on existing regulations to address the complexities and ensure both the protection of individuals' rights and the effectiveness of law enforcement efforts. Cyber- physical systems, integrating computing and communication with physical systems, herald a new era of interaction and manipulation of our surroundings. Recognizing their transformative potential, significant global investments are being made to develop this technology, paving the way for a more connected and responsive physical world [45]. A review given in [46] explores the pivotal role of sensor and actuator technologies in advancing smart city development, addressing key aspects such as technological advancements, data security, regulatory frameworks, and future prospects. The study in [47] provides a comprehensive analysis of how computer vision technologies have transformed product design and development, exploring its historical context, applications, and implications. Through an examination of multiple datasets and thematic studies, the findings underscore the significant impact of computer vision on design processes and highlight key areas for future research and innovation in this evolving field.

The security challenges facing Internet-of-Things (IoT) de- vices, emphasizing the need for lightweight authentication and data integrity solutions to safeguard these resource-constrained devices is presented in [48]. Through analysis of various lightweight protocols and their vulnerabilities, the study high- lights the importance of mitigating security threats such as man-in-the-middle attacks, replay attacks, and denial of service attacks, while also discussing the utility of the Microsoft threat modeling tool for IoT applications. In [49], the authors proposed a solution to address the significant issue of driving under the influence,

BACTmobile introduces a fully automated, secure Blood Alcohol Concentration (BAC) Tracking System for vehicles. Utilizing physiological, psychological, and physical behavior data, it accurately detects and predicts BAC levels, ensuring road safety with a demonstrated model accuracy of 99The review paper [50] paper conducts a systematic analysis of state-of-the-art voice Presentation Attack Detection (PAD) systems to address the vulnerability of biometric technology to spoofing attacks. Through a survey of 172 articles published between 2015 and 2021, it identifies areas for further research and highlights the need for advancements in spoof-type independent PAD systems.

A novel security scheme for fog computing architectures, utilizing physical unclonable functions (PUFs) to enable secure authentication without manual user interaction is introduced in [51]. The proposed scheme ensures anonymity, unlikability, perfect forward secrecy, and resistance against stolen device attacks, while maintaining efficient performance through symmetric key-based operations. In [52], the authors proposed the AMEVCC scheme to address latency issues in vehicular applications by leveraging fog computing, ensuring mutual authentication and anonymity for secure message exchange. The protocol's security and efficiency are validated through computational cost analysis and formal proofs in the random oracle model. An improved authentication protocol for smart grid environments to address vulnerabilities found in a recent three-factor authentication (3FA) scheme by Wazid et al is proposed in [53]. The scheme is formally verified using the ProVerif tool and shown to provide enhanced security features compared to existing protocols. The paper [54] reviews security vulnerabilities, threats, and attacks in the robotics domain, high- lighting the need for enhanced security measures. It proposes multi-factor authentication schemes and cryptographic algorithms to improve the security of robotic systems. The review in [55] and [56] discusses self-powered sensing systems augmented with machine learning for large-scale deployment in the internet of things (IoT), highlighting challenges such as stable power harvesting and privacy concerns. It also presents principles for self-powering sensors and recent progress in applying machine learning techniques to enhance their capabilities, outlining potential research needs and future directions. In [57], the authors introduce a redesigned Generative Adversarial Network (GAN) model, Convolutional Long short-term GAN (CLGAN), which combines long short-term memory (LSTM) and a convolutional neural network (CNN) to accurately identify individual drivers and detect vehicle theft. By leveraging a public dataset collected from in-vehicle Controller Area Network (CAN) bus, the proposed CLGAN model achieves high accuracy of 98.5 pec and demonstrates robustness against various driving conditions on multiple types of roads. The study in [58] proposed an optimized IoT architecture, called Face Recognition and Emotion Detection based on IoT (FRED-IoT), to track drivers' emotional states and perform face recognition in autonomous vehicles. By leveraging wireless transmission of physiological signals to a centralized database management center, FRED- IoT achieves a low delay of 2 milliseconds and significantly improves reliability, attaining a high F-score of 96 pec.

In [59], the authors comprehensively examine detection methods for smart vehicles across various communication net- works, including in-vehicle networks, inter-vehicle networks, ground vehicle power stations, and the Internet of Drones (IoD). Analyzing studies published between 2018 and 2022, the paper evaluates intrusion detection systems (IDSs), anomaly detection, attack detection, and hybrid detection methods, ad- dressing research questions and discussing future challenges in securing smart vehicles. A survey in [60] offers a com- prehensive overview of the application of machine learning for cyber threat detection in IoT environments, including a comparative analysis of state-of-the-art ML-based Intrusion Detection Systems (IDSs). It addresses unresolved issues and presents a future vision for enhancing IoT security using Generative AI and large language models, serving as a valuable resource for researchers and practitioners in this evolving field. The researchers in [61] introduced a lightweight authentication and key management (L-AKM) scheme for Smart IoT-Assisted Systems, addressing challenges in ensuring end-to-end security and perfect secrecy in LoRa-WAN communication. Through continuous authentication and session management, L-AKM enhances security efficiencies and resilience against potential attacks, albeit with some trade-offs in transmission delay and throughput rate, as observed in experimental analysis. The paper [62] proposed DivaCAN, a novel intrusion-detection methodology for securing in-vehicle communication on the CAN protocol. Leveraging an ensemble of classifiers, DivaCAN demonstrates exceptional performance with a precision of 94.93 pec, a recall of 94.98 pec, and an F1 score of 94.97 pec, while emphasizing a low false-positive rate and maintaining acceptable execution time.

In [63], the authors introduced a decentralized Attribute-based Authentication (ABA) protocol for wearable-based Col- laborative Indoor Positioning Systems (CIPSs), offering enhanced privacy protection and untraceability compared to existing centralized protocols like iBeacon. Through extensive experimentation, the proposed protocol demonstrates practicality and feasibility for real-world deployment, paving the way for secure and privacy-preserving CIPSs in the expanding realm of Internet of Things (IoT) applications. The research in [64] aims to enhance safety and security management in cyber-physical systems by introducing TOMSAC, a practical methodology for managing interdependencies and trade-offs throughout the development process. TOMSAC offers a user-friendly approach to address safety and cybersecurity concerns, providing a com- prehensive framework for decision-making and risk mitigation. FogHA, an anonymous handover authentication scheme for fog computing, ensuring mutual authentication and key agreement between fog nodes and mobile devices is introduced in [65]. FogHA boasts high handover efficiency, lightweight crypto- graphic primitives, and proven security through formal analysis, outperforming existing schemes in terms of communication and computation costs while resisting known attacks. The survey in [66] explored cryptographic techniques proposed for achieving authentication, privacy, and security in Vehicular Ad- Hoc Networks (VANETs), including symmetric and public key cryptography, identity-based and pseudonym-

based schemes, as well as blockchain-based approaches. The study identifies existing challenges such as reliance on trusted authorities, heavy computation for certificate revocation, and significant over- head affecting timely message delivery, emphasizing the need for lightweight and efficient privacy-preserving authentication schemes in VANETs.

The research in [67] provides a comprehensive survey of authentication aspects in IoT and related domains, assessing existing approaches and identifying their limitations. It offers a novel multidimensional perspective, connecting evolution of solution strategies and outlining future research directions, serving as a valuable resource for academia and industry seeking insights into IoT authentication schemes. The survey in [68] explores the deployment of authentication and access control methods via Distributed Ledger Technology (DLT) across various networking use cases, addressing challenges of centralized solutions and proposing a taxonomy for categorization. While DLT offers promising benefits, challenges persist for the migration to DLT-based AAC, prompting discussion on future directions to address current gaps and future needs.

In [69], the authors introduced a hybrid vehicular edge computing solution aimed at enhancing communication effectiveness by facilitating frequent vehicle-to-edge server inter- action without reliance on trusted intermediaries. Through a formal security proof, the proposed framework ensures security, message integrity, and privacy in edge-based vehicular communications, demonstrating superior efficiency compared to conventional cloud computing frameworks. The research in [70], provides a comprehensive analysis of blockchain-based multi-factor authentication (BMFA) and proposes a BMFA-as- a-service (BMFAaaS) approach, outlining key implementation requirements based on a systematic literature review conducted from 2019 to 2023. It addresses the need for robust authen- tication mechanisms in increasingly sophisticated distributed systems like IoT, Fog, and WSN, while also discussing research challenges and future directions for BMFAaaS. The trends in biometric technology based on patent documents from 1990 to 2016, revealing rapid advancements in fingerprint-enabled car anti-theft systems and increasing popularity of biometric signal transmitting models is analysed in [71]. Despite ongoing progress in fingerprint, face, and iris authentication, other technologies such as finger vein, voice, and signature authentication are trailing behind, while biometric applications in financial transactions and digital media content security are declining. A systematic review of Machine Learning and Deep Learning-based user authentication and authorization, exploring application domains, datasets, algorithms, and challenges is performed in [72]. The study offers a comprehensive overview and outlines future research directions, serving as a valuable resource for interdisciplinary studies in cyber security. A novel approach to decentralized authentication for smart homes by integrating fog computing with blockchain technology is pro-vided in [73]. Through formal and informal security analysis, the proposed scheme demonstrates improved security properties and performance compared to existing solutions, addressing challenges such as resource constraints and security concerns in the distributed smart home environment. The research in [74] presents a three-factor authentication and key-sharing protocol for IoT devices, integrating physical unclonable function (PUF) technology to enhance security against attacks like device cloning and key tampering. Through computational analysis and comparison with existing protocols, our proposed scheme demonstrates superior security properties and efficiency, making it suitable for resource-constrained IoT environments.

The article in [75] provides a comprehensive overview of security challenges in IoT applications, emphasizing the need for robust security measures such as end-to-end encryption and authentication. It explores various technologies, including machine learning, fog computing, edge computing, and blockchain, aimed at enhancing security and trust in IoT environments. The proposed vehicle ignition system in [76] utilizes dactylogram scanning for authorized access, allowing only enrolled individuals to start the vehicle. Equipped with GSM capability, the system promptly alerts the vehicle owner via SMS in case of unauthorized access attempts. A Biometric-based User Authentication and Key Agreement Protocol (BUAKA) tailored for resource-constrained ad hoc networks, addressing limitations of conventional security solutions is presented in [77]. Through the use of fuzzy extractors and one-way hash functions, BUAKA offers a lightweight yet secure authentication mechanism, effectively mitigating various security threats while minimizing resource consumption. In [78], a novel protocol for the Internet of Vehicles (IoV) that integrates biometric-based user authentication and Physical Unclonable Function (PUF) technology to enhance security against various attacks is presented. Through informal and formal analyses, including RoR model and Scyther tool verification, our protocol demonstrates robust security features and low computation time, making it suitable for secure communication within IoV systems. The review in [79] examines the integration of artificial intelligence (AI) with biometrics to bolster security measures, particularly in the context of the Internet of Things (IoT), offering insights into their synergies and potential applications. By enhancing pattern recognition and decision-making capabilities, AI-powered biometrics contribute to improved authentication methods in IoT environments, mitigating security risks and safeguarding user privacy.

A secure authentication framework for Vehicular Cloud Net- working (VCN) based on elliptic curve cryptography (ECC) and biometrics, ensuring security, privacy, and integrity in communications is introduced in [80]. Through formal and informal analysis, as well as simulation using AVISPA, the proposed protocol demonstrates efficacy against various attacks and is shown to be both secure and efficient compared to similar protocols, making it suitable for VCN applications. PASKE-IoD, a Privacy-Protecting Authenticated Session Key Establishment (ASKE) scheme for the Internet of Drones (IoD), ensuring secure communication between drones and external users is given in [81]. Through informal security analysis and verification using Scyther, as well as Burrows-Abadi-Needham logic, PASKE-IoD demonstrates resilience against security attacks and offers enhanced security features compared to existing ASKE schemes.

III. PREPARE YOUR PAPER BEFORE STYLING

The landscape of intelligent transportation systems has under- gone significant evolution in recent decades, with the integration of advanced technologies enhancing security, connectivity, and automation. However, this technological advancement has also introduced new challenges, particularly the rising threat of unauthorized vehicle access and cyber-physical attacks. Innovations such as smart networking, GPS-enabled navigation, and keyless entry systems have increased the vulnerability of modern vehicles to cyber threats, necessitating robust security mechanisms. The automotive industry has responded to these challenges by continuously developing and deploying sophisticated security architectures, ranging from traditional mechanical locks to state-of-the-art biometric authentication systems. This dynamic evolution underscores the critical role of vehicle security systems in safeguarding intelligent transportation networks from emerging threats, requiring continuous adaptation and innovation. The consequences of vehicle theft extend beyond economic losses, as they pose significant risks to public safety, contribute to criminal activities, and compromise transportation infrastructure integrity. The need for robust vehicle security systems is, therefore, imperative to ensure the protection of assets and maintain secure mobility solutions. In the context of evolving cybersecurity threats, collaborative efforts among researchers, policymakers, and industry stakeholders play a pivotal role in enhancing vehicle security frameworks. The increasing reliance on interconnected vehicular networks demands proactive security measures to mitigate unauthorized access and exploitation by adversaries.

Traditional vehicle access methods, such as key fobs and remote unlocking systems, were once considered secure. How- ever, rapid advancements in wireless communication and cryptographic techniques have introduced vulnerabilities that adversaries can exploit. One prevalent attack vector is signal interception, where attackers eavesdrop on the radio frequency signals transmitted between a key fob and the vehicle, enabling unauthorized access. Another major threat is code grabbing, wherein attackers capture encrypted signals and decode them to bypass authentication mechanisms [5], [6]. Replay attacks involve recording and retransmitting authentication signals at a later time to deceive vehicle security systems, while key cloning techniques allow unauthorized duplication of access credentials due to weak encryption standards. Additionally, jamming attacks disrupt communication between the key fob and the vehicle, preventing owners from securing their vehicles. Once inside the vehicle, adversaries can exploit vulnerabilities in the Electronic Control Unit (ECU) via the On- Board Diagnostics (OBD) port, manipulating critical vehicular functions and bypassing immobilization systems. These emerging attack methodologies necessitate the development of innovative security paradigms to reinforce vehicular authentication mechanisms. The integration of biometric authentication within vehicle security frameworks represents a transformative approach to addressing these challenges. Biometric systems leverage unique physiological characteristics such as fingerprint recognition, iris scanning, and facial recognition to establish highly secure, user-specific authentication protocols [7]. Unlike traditional access methods, biometric authentication enhances security by ensuring that only authorized users can operate the vehicle, thereby significantly reducing unauthorized access risks. Additionally, biometric authentication streamlines the access process, eliminating the dependency on physical keys or memorized credentials. These systems can be seamlessly integrated into vehicle access points, including door locks, ignition mechanisms, and autonomous driver authentication modules, enhancing both security and usability. The inherent uniqueness of biometric data serves as a deterrent against theft and unauthorized usage, reinforcing vehicle security in interconnected transportation ecosystems.

Future advancements in biometric authentication may incorporate multi-modal security mechanisms, combining fingerprint and iris-based authentication with cryptographic enhancements to mitigate emerging threats. However, despite its advantages, biometric authentication faces certain limitations that must be addressed to ensure widespread adoption in automotive applications. One critical challenge is the susceptibility to false positives and false negatives in biometric recognition, which may arise due to environmental conditions, physiological variations, or sensor inaccuracies [8], [9]. For instance, changes in user biometrics due to injuries or unfavorable lighting conditions may hinder authentication accuracy. Additionally, concerns surrounding privacy and data security pose significant ethical and legal challenges, as biometric data storage and processing require stringent protection against potential breaches or misuse. The cost of integrating biometric authentication within vehicles also presents an economic barrier, particularly for cost-sensitive consumer markets. Furthermore, like other digital security systems, biometric authentication mechanisms must remain resilient against adversarial attacks, including spoofing and deepfake-based impersonation. Continuous advancements in cybersecurity protocols and secure data encryption are essential to ensuring the integrity and reliability of biometric authentication frameworks. The implementation of iris and fingerprint-based authentication in vehicular security addresses a fundamental requirement in the domain of intelligent transportation. By leveraging advanced biometric technologies, this approach enhances vehicle access security while mitigating the limitations of conventional methods. The adoption of multi- factor authentication, combining fingerprint and iris recognition, significantly strengthens security against adversarial access at- tempts. Beyond conventional vehicle security applications, bio- metric authentication holds immense potential in autonomous and connected vehicle ecosystems, where secure identity verification is crucial for driver authorization and operational safety. The integration of sophisticated biometric authentication mechanisms within autonomous vehicle architectures ensures secure human-machine interaction and access control, aligning with advancements in self-driving and robotic transportation systems.

This research contributes to the ongoing development of authentication systems in both vehicular security and broader biometric applications. By evaluating the cybersecurity implications of integrating biometric technologies, the study

enhances the resilience of vehicular authentication frameworks against emerging threats. Furthermore, it lays the foundation for future advancements in intelligent transportation security, fostering innovation in access control systems and autonomous vehicle authentication mechanisms. Ultimately, the exploration of iris and fingerprint-based authentication not only fortifies contemporary vehicle security but also paves the way for the next generation of secure, interconnected mobility solutions.

IV. METHODOLOGY

Enhancing vehicle security necessitates the exploration of advanced authentication mechanisms to replace conventional key fob systems, which remain susceptible to a wide range of security vulnerabilities. One promising alternative is bio- metric authentication, which leverages unique physiological characteristics to ensure robust and reliable access control. Biometric systems offer an inherent advantage in security due to the distinctiveness of individual biometric traits, making them significantly harder to forge or replicate. However, a unimodal biometric system may not provide optimal security and usability, necessitating the integration of a dual biometric approach that combines two independent authentication modal- ities. This methodology enhances security while maintaining high system reliability and user satisfaction. Among the various biometric techniques available, fingerprint scanning and iris recognition have demonstrated superior accuracy, affordability, and practicality for automotive applications. These technologies have undergone extensive research and development, resulting in their economic feasibility for large-scale deployment in vehicular security systems. Fingerprint recognition is widely regarded for its speed and non-intrusive nature, allowing seamless vehicle access without physical keys. Similarly, iris recognition offers a high level of security due to the complex, unique pattern of the iris, which remains stable over time and is nearly impossible to duplicate [5], [7]. Integrating these biometric technologies into vehicular access control enhances security by eliminating key fob-related threats, such as cloning and relay attacks, while providing a user-centric and intuitive experience. By adopting a multimodal biometric authentication system, manufacturers can significantly reduce unauthorized vehicle access while improving user convenience, aligning with the broader trend of secure and intelligent transportation systems. The capacitive fingerprint sensor has been selected due to its robustness in diverse environmental conditions. Unlike optical or ultrasonic fingerprint sensors, capacitive sensors do not rely on specific lighting conditions, making them highly suitable for vehicular applications. These sensors operate by

detecting the electrical charge variations produced by finger- print ridges and valleys, ensuring high-resolution imaging and resistance to spoofing attacks [8]. Moreover, their durability, cost-effectiveness, and accuracy make them ideal for automotive security. To maximize both usability and protection, the fingerprint sensor is strategically embedded within the inner surface of the vehicle's door handle. This placement safeguards the sensor from external damage while providing natural user interaction—drivers authenticate themselves simply by gripping the handle, eliminating additional steps and minimizing authentication time. Positioning the sensor within a pull-out door handle—common in modern vehicle designs—ensures seamless integration without compromising aesthetics or ergonomics. The larger surface area of the handle facilitates effective sensor embedding while maintaining the functional integrity of the vehicle. This integration enhances the overall user experience, making biometric authentication both intuitive and secure, reducing friction in daily use, and reinforcing advanced biometric security mechanisms for vehicular access.

Iris recognition serves as a complementary biometric modality, ensuring authentication redundancy in cases where finger- print scanning may be impractical, such as when users wear gloves in cold environments. The iris scanner captures high- resolution images of the user's iris using near-infrared imaging technology, enabling precise identification across variable lighting conditions and moderate distances [9]. For optimal usability, the iris scanner is installed within the A or B-pillar of the vehicle, ensuring that drivers can effortlessly align their eyes with the scanner upon entry or while seated inside. This placement minimizes user inconvenience while ensuring high authentication accuracy. The resilience of iris recognition technology to ambient light variations makes it particularly suitable for vehicular security applications, ensuring consistent performance in varying operational environments. The hardware implementation of the dual biometric authentication system is depicted in Fig. 2. The fingerprint sensor and iris scanner capture raw biometric data, which is subsequently transmitted to a central microprocessor for real-time processing and matching. The system architecture incorporates a dedicated memory unit and an image processing module. The memory unit securely stores registered biometric templates, facilitating authentication by comparing new inputs against stored reference data. The image processing module plays a crucial role in converting raw biometric signals into digital representations suitable for analysis. It transforms analog sensor outputs into structured data formats that can be efficiently processed by the microprocessor, ensuring seamless integration of both biometric modalities. Upon receiving formatted biometric data, the microprocessor performs authentication by executing a matching algorithm. If the input biometric data aligns with stored templates, vehicle access is granted. In cases of authentication failure, the system prompts a reattempt to mitigate false negatives. The image processing software is instrumental in enhancing iris recognition accuracy, converting captured images into standardized digital patterns that are stored securely in the vehicle's database. Each authentication attempt triggers a comparison between the live biometric data and pre-registered patterns, ensuring reliable and secure access control.

The integration of fingerprint and iris-based authentication within the vehicle security framework is orchestrated by a central embedded controller equipped with onboard memory. This controller not only manages biometric data processing but also implements access control logic to regulate vehicle entry based on authentication outcomes. By leveraging the unique physiological characteristics of users, the system offers a significantly higher security standard compared to traditional key-based mechanisms. Furthermore,

it eliminates the risks associated with key fob interception, cloning, and relay attacks, providing a resilient defense against emerging cybersecurity threats [6]. This dual biometric approach represents a trans- formative advancement in vehicular security, aligning with the broader objectives of autonomous vehicle authentication and intelligent transportation security. By integrating advanced bio- metric modalities within vehicular architectures, this method- ology enhances not only security but also user convenience, reinforcing the role of robotics and artificial intelligence in next- generation transportation systems.

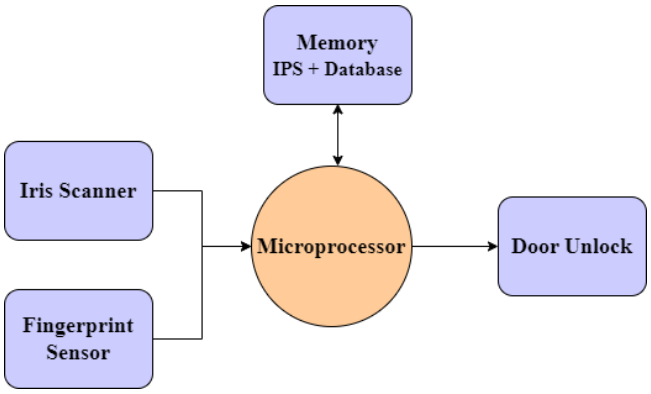

Fig. 2. Hardware components, the microprocessor compares the input biometrics with the ones in database and actuates the door lock

To enhance security and mitigate the risk of fraudulent biometric attempts, a robust authentication logic is implemented within the vehicle's security system. This logic, as depicted in Fig. 3, employs a multi-layered approach to ensure that unauthorized access attempts are effectively detected and prevented. The system utilizes a multimodal biometric authentication approach, incorporating multiple biometric modalities for access control. While both fingerprint and iris recognition systems are integrated, a single authentication mode is typically sufficient for vehicle access. Initially, the system permits authentication via either fingerprint or iris scanning within the first three authentication attempts. If the user fails to authenticate within these attempts using either method, a simultaneous fingerprint and iris scan is mandated for further authentication.

Biometric inputs are processed and matched against registered templates stored in the onboard memory of the vehicle's central microprocessor. If no match is found, the system prompts the user for a rescan. After three unsuccessful attempts, the system escalates security measures by enforcing a dual biometric authentication process requiring both fingerprint and iris verification. Upon successful authentication, the system grants access to the vehicle. The core principle of this authentication logic involves establishing predefined thresholds and fallback mechanisms based on failed authentication attempts. Specifically, if fingerprint or iris authentication fails three consecutive times, the system automatically transitions to a dual authentication process requiring both modalities for successful verification. This additional security layer significantly mitigates the likelihood of unauthorized access using spoofed or forged biometric data. Moreover, the authentication logic includes contingency measures to handle failed authentication scenarios. If an initial biometric scan fails due to environmental factors such as poor lighting, sensor contamination, or user misalignment, the system prompts for a rescan rather than outright denying access. This dynamic error-handling mechanism enhances the user experience by allowing occasional authentication inconsistencies without compromising security.

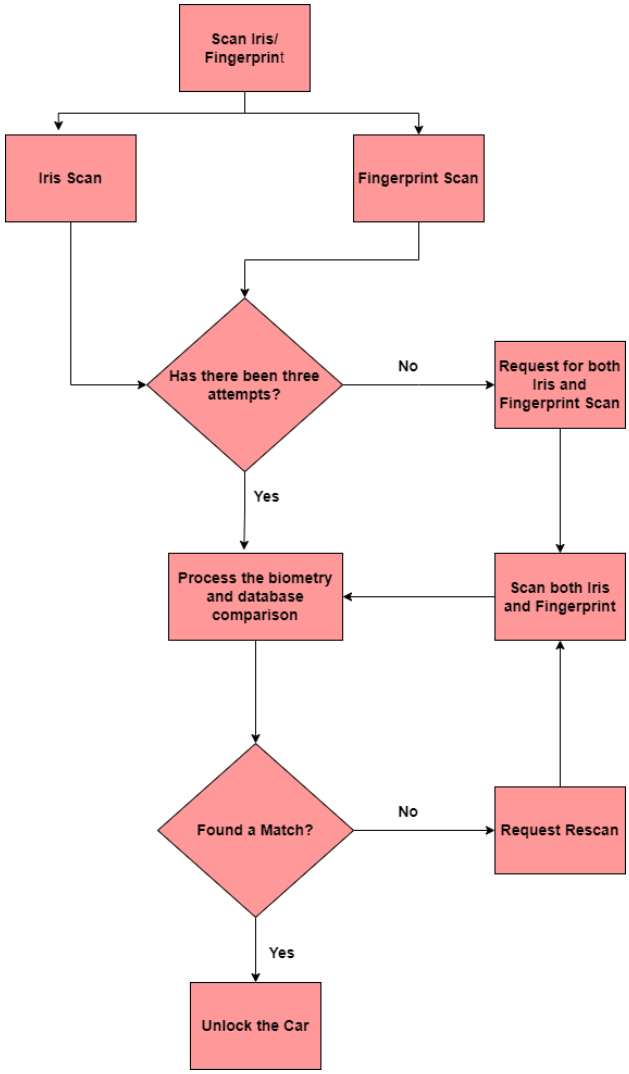

Fig. 3. Logic implemented for improved security

By adhering to this structured authentication logic, the vehicle can only be accessed through validated biometric data, either via an independent scan or a mandatory dual authentication process following repeated failures. This stringent protocol ensures that only genuine, registered biometric profiles can unlock the vehicle, effectively preventing security breaches involving counterfeit or replicated biometric credentials. The integration of such a sophisticated authentication logic underscores the commitment to both security and user convenience in mod- ern vehicle access systems. By leveraging advanced biometric technologies alongside intelligent authentication protocols, automotive manufacturers can elevate vehicle security standards, offering enhanced protection while maintaining seamless accessibility and user experience. An algorithm showcasing the methodology followed is given in 1.

The adoption of biometric authentication technologies in vehicles presents a significant advancement in enhancing vehicle safety, security, and convenience. By replacing traditional key- based systems with biometric solutions such as fingerprint and iris scanners, automakers can not only streamline user access but also potentially lower the overall cost of vehicle security systems. This reduction in cost stems from the elimination of the need for physical keys, which can be expensive to replace in cases of loss or damage. Focusing specifically on the finger- print scanner, further optimization for automotive applications can greatly improve its functionality. By designing fingerprint scanners that are better suited to withstand outdoor automotive environments, such improvements can enhance both the speed and accuracy of scans. This results in quicker vehicle access, allowing drivers to enter and start their vehicles more efficiently without compromising security. Similarly, advancements in iris scanning technology can be tailored specifically for use in vehicles. Enhancements can include improving the scanner's ability to capture high-quality images under varied lighting conditions typical of automotive settings. Optimizing iris scan- ners for quicker and more reliable performance ensures that they can serve as a dependable method of user authentication. Moreover, integrating these biometric systems into the vehicle's ignition switch offers a robust two-level authentication process. This means that a driver must successfully authenticate via the biometric system not only to unlock the car but also to start the engine. Such integration adds an additional layer of security, ensuring that even if unauthorized access to the vehicle occurs, starting and driving the vehicle remains secure against unauthorized use. Overall, the integration of biometric technologies into vehicle systems transforms the security landscape by offering a more secure, convenient, and cost-effective alternative to traditional car keys. This approach not only enhances the user experience but also aligns with modern technological advancements in vehicle security.

The strategic placement of the biometric scanners—specifically the fingerprint and iris scanners—is paramount in ensuring that the system is not only secure but also user-friendly and ergonomic. This thoughtful positioning facilitates easy and natural access, integrating seamlessly into the vehicle's design to enhance both security and user experience. The fingerprint scanner is ingeniously incorporated into the inner side of the driver-side door handle. This placement leverages the natural motion of reaching for the door handle as an opportunity for authentication, making it both intuitive and efficient. The scanner is designed to capture an extensive area, accommodating not just the fingerprints but also part of the palm. This dual capture approach significantly enhances the system's security capabilities by increasing the uniqueness of each biometric scan, thereby reducing the likelihood of unauthorized access. Conversely, the iris scanner is optimally positioned towards the B-pillar of the vehicle. This location is specifically chosen to align with the driver's eye level as they enter the car or adjust their seating position, ensuring that the process of iris scanning is as unobtrusive as possible. The scanner's placement at either the apex of the door frame or within immediate proximity of the driver's entrance minimizes the need for the driver to make any awkward movements, thereby adhering to ergonomic principles while maintaining high security standards. Further elaboration on these strategic placements can be found in Fig. 4, which shows the exact locations of the biometric scanners within the vehicle's architecture. This illustration not only shows where each scanner is located but also explains why these specific locations were chosen. The rationale behind this design strategy focuses on maximizing ease of use, security, and efficiency, ensuring that the authentication process is as seamless as possible without compromising the vehicle's aesthetic or functional integrity. By incorporating these advanced biometric systems strategically within the vehicle, manufacturers can offer a superior blend of accessibility, security, and user comfort, ultimately enhancing the overall vehicle ownership experience.

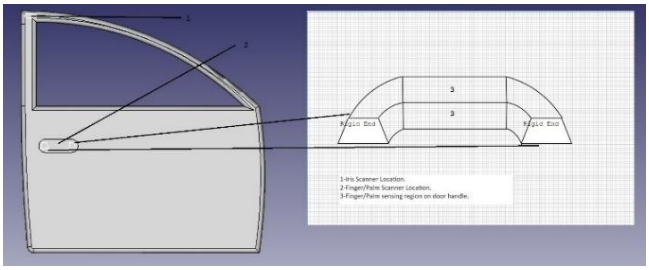

Fig. 4. Positioning of Iris and Fingerprint Sensors

Algorithm 1. Dual Biometric Authentication for Vehicle Access

```
   Input: Fingerprint scan F, Iris scan I
Output: Vehicle access granted or denied
Initialize attempt counter A ← 0
   Initialize authentication flag
Authenticated ← False
   while A < 3 and Authenticated == False
do User attempts authentication using
either F or I if F matches stored
fingerprint template, then
   Authenticated ← True
   else if I match stored iris template
then
   Authenticated ← True
   else
   Increment attempt counter: A ← A + 1
   end if end while
   if Authenticated == False then
   Require dual authentication: User must
scan both F and
   I
   if F matches stored template AND I
match stored template
   then
   Authenticated ← True
   else
   Access denied Trigger security alert
   end if end if
   if Authenticated == True then
   Grant vehicle access
   else
   Deny access and log failed attempt
   end if
```

V. DESIGN APPROACH

The sophisticated design of the sensor placement and functionality in this vehicle security system is carefully crafted to achieve two crucial objectives: enhancing user convenience and strengthening security measures. This system incorporates advanced authentication processes that are seamlessly integrated into the vehicle's architecture, ensuring robust security against a wide range of environmental challenges and varied usage scenarios. To optimize user convenience, the sensors are strategically located where interactions naturally occur, such as the inner side of the driver-side door handle for the fingerprint scanner, and the B-pillar for the iris scanner. This strategic placement leverages routine user movements, allowing for effortless authentication as drivers engage with the vehicle—whether gripping the door handle or aligning with the vehicle's entry point. This integration ensures that the process of securing and starting the vehicle is as intuitive as pulling a door handle or glancing at a mirror. Simultaneously, the system is engineered to fortify vehicle security. It employs state- of-the-art biometric technology capable of high accuracy and rapid processing, minimizing the risk of unauthorized access. Moreover, these biometric scanners are designed to withstand various environmental factors such as extreme temperatures, humidity, and lighting conditions that might otherwise impede their functionality. The resilience of these systems ensures reliable performance regardless of whether the vehicle is parked outdoors in harsh weather or in the fluctuating conditions of a garage. By integrating these advanced technologies, the vehicle security system not only offers a seamless user experience but also maintains a vigilant guard against potential security breaches. This dual focus on convenience and security not only enhances the user experience but also positions the system as a forward-thinking solution in automotive security technology. At the heart of the vehicle security system's design philosophy is a sophisticated, multi-faceted authentication strategy, intricately integrated into the overall framework. This approach utilizes a dual-authentication model, harnessing the strengths of both fingerprint and iris scanning technologies. Known for their exceptional accuracy and the unique biometric features inherent to each individual, these methods offer a superior level of security. The combination of fingerprint and iris scanning technologies is central to creating a robust barrier against unauthorized access. Fingerprint scanners capture the intricate details of a person's fingerprint, which are nearly impossible to replicate due to the unique patterns of ridges and valleys on each finger. On the other hand, iris scanning technology analyzes the complex patterns of a person's iris, which are equally distinctive and remain stable throughout one's life. By leveraging these biometric systems, the vehicle security system capitalizes on the physical attributes that are uniquely and permanently tied to the owner. This dual-node authentication system is designed to operate effectively across a wide range of environmental conditions. Whether in bright sunlight, low light, or under adverse weather conditions, the system's advanced sensors are equipped to perform reliably. This resilience ensures that the biometric authentication process remains consistent and secure, providing peace of mind for vehicle owners. Furthermore, integrating these two sophisticated biometric technologies enhances security by requiring that both biometric identifiers match their stored templates before granting access. This layered security approach significantly reduces the risk of false entries and unauthorized access, ensuring that the vehicle remains secure in virtually any scenario. By adopting this comprehensive, integrated authentication process, the vehicle security system not only provides enhanced security but also offers a seamless and user-friendly access experience, making it a cutting-edge solution in the landscape of automotive security technologies.

The cornerstone of our design strategy lies in the strategic deployment of sensors, meticulously calibrated and positioned to optimize functionality within the vehicle security system. These sensors are strategically placed to align with the natural movement patterns and interaction points of users, ensuring seamless integration with human behavior and fostering intuitive engagement and satisfaction. This ergonomic approach to sensor placement is designed to enhance operational efficiency while alleviating user fatigue. By carefully considering how users interact with the vehicle, we ensure that accessing and utilizing the security system feels instinctive and effortless. For example, placing the fingerprint sensor on the inner side of the driver-side door handle aligns with the natural motion of reaching for the handle when entering the vehicle. Similarly, positioning the iris scanner near the B-pillar of the car corresponds with the driver's line of sight as they approach or exit the vehicle. By aligning sensor placement with user behavior, we not only enhance usability but also improve overall satisfaction with the vehicle. Users can engage with the security system seamlessly, without needing to learn or adapt to unfamiliar processes. This intuitive design fosters a positive user experience, contributing to greater satisfaction and loyalty among vehicle owners. Moreover, this ergonomic approach also contributes to safety by minimizing distractions and reducing the need for users to divert their attention away from the task at hand. By streamlining the authentication process and integrating it seamlessly into the vehicle's design, we prioritize both usability and safety, creating a holistic approach to vehicle security that enhances the overall driving experience.

In our pursuit of innovation, we have identified the Mantra MIS100V2 Iris scanner showcased in Fig. 5 as a pivotal component of our design. This state-of-the-art scanner boasts a compact design and seamless compatibility with popular operating systems, making it an ideal candidate for integration into vehicles. Its compact form factor ensures optimal positioning within the vehicle without compromising functionality.

Moreover, the design of the sensor can be customized to facilitate easy incorporation into the vehicle's architecture, ensuring a seamless blend with the overall design aesthetic. Additionally, our design incorporates a custom capacitive sensor strategically placed on the inner side of the door handle. This sensor revolutionizes the authentication process by offering an expansive scanning area, thereby guaranteeing heightened security and accuracy. Unlike traditional sensors, which may struggle with partial prints, this innovative capacitive sensor is capable of swift authentication even

when presented with incomplete or partial fingerprints. By leveraging these cutting- edge technologies, our design not only enhances the security of the vehicle but also prioritizes user experience and convenience. The seamless integration of advanced biometric sensors ensures that vehicle access is both secure and effortless, providing users with peace of mind while enriching their overall driving experience. With a focus on innovation and user-centric design, our approach sets a new standard for automotive security systems, paving the way for safer, more intuitive vehicle access solutions.

Fig. 5. Mantra MIS100V2 Iris Scanner

While security remains paramount, our design approach places equal emphasis on usability and comfort. The multimodal authentication process seamlessly integrates high-level biometric security with user convenience, ensuring a harmonious balance of functionality and ease of use. In essence, our design approach embodies a harmonious synthesis of innovation and user-centric principles. By meticulously orchestrating sensor placement and authentication methodologies, we transcend conventional boundaries, delivering a solution that not only meets but exceeds the expectations of modern-day users. Through a seamless blend of convenience, security, and ergonomic excellence, we pave the way for a new era in vehicle security systems. Our commitment to usability and comfort ensures that users can interact with the security system effortlessly, without compromising on security. By prioritizing both security and user experience, we create a solution that not only safeguards vehicles but also enhances the overall driving experience. With a focus on innovation and user-centric design, our approach sets a new standard for automotive security systems, elevating the expectations of what is possible in the realm of vehicle security.

VI. CONCLUSION AND FUTURE DIRECTIONS

This paper presents a novel vehicle security system designed to improve both convenience and security by addressing vulnerabilities inherent in traditional key fobs or keycards. The system incorporates advanced biometric authentication techniques, specifically fingerprint and iris recognition, to deliver robust and dependable access control. At the heart of the design lies the principle of multi-nodal authentication, where both fingerprint and iris scans are employed under certain circumstances, such as repeated failed authentication attempts or extended periods of inactivity. Under typical conditions, authentication using either modality is sufficient for vehicle access, ensuring a smooth user experience while maintaining security. The system's affordability and efficiency are paramount, achieved through the integration of a specialized capacitive sensor tailored for outdoor conditions, seamlessly embedded within the inner side of the pull-out door handle. Additionally, the integration of a compact and accurate iris scanner, such as the MantraMIS100V2, enhances accessibility and reliability, establishing the solution as a compelling substitute for traditional vehicle access systems. Furthermore, the deliberate placement of these sensors optimizes user interaction by enabling effortless access and ensuring the security system's optimal performance. While the proposed system offers significant advancements in vehicle security technology, we recognize several limitations and challenges that warrant further investigation. Environmental factors such as extreme weather conditions (heavy rain, snow, dirt accumulation), sensor contamination, and hardware malfunctions may affect the reliability and accuracy of both fingerprint and iris recognition systems. The possibility, albeit low, of simultaneous failure of both biometric modalities necessitates the development of robust fallback mechanisms to maintain system accessibility without compromising security. Additionally, integrating dual biometric systems introduces considerations related to computational overhead and energy consumption, which are particularly critical for electric and hybrid vehicles where energy efficiency directly impacts performance and sustainability. Future work will focus on optimizing the system's processing algorithms to reduce power requirements and implementing adaptive authentication protocols that dynamically balance security and usability based on contextual factors.

Expanding the design's applicability to various handle designs, such as push-in and touch door handles, presents opportunities for optimization. These designs allow minimal palm con- tact, necessitating efficient fingerprint data acquisition within a limited time frame. Moreover, fingerprint technology could be adapted for flap-type door handles, sharing functional similarities with the pull-out handles considered here. By addressing these challenges through ongoing research and development, this methodology aims to realize safer, more reliable, and user-friendly vehicle access solutions. The integration of state- of-the-art biometric technologies within intelligent transportation systems represents a significant stride toward secure and convenient autonomous mobility, with potential applications extending beyond vehicular security.

ACKNOWLEDGMENT

The authors would like to thank Manipal Institute of Technology, MAHE Manipal for providing the facilitates required for this research.

REFERENCES

[1] G. B. Loganathan, "CAN Based Automated Vehicle Security System," *International Journal of Mechanical Engineering and Technology*, vol. 10, no. 7, 2019.

[2] P. Singh, T. Sethi, B. K. Balabantaray, and B. B. Biswal, "Advanced vehicle security system," in *ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems*, pp. 1–6, 2015, doi: 10.1109/ICIIECS.2015.7193276.

[3] R. Prashantkumar, S. Sagar, Nambiar, and Siddharth, "Two-wheeler vehicle security system," *International Journal of Engineering Sciences and Emerging Technologies*, pp. 324–334, 2013.

[4] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proceedings - IEEE Symposium on Security and Privacy*, pp. 447–462, 2010, doi: 10.1109/SP.2010.34.

[5] R. Prashantkumar, S. Sagar, Nambiar, and Siddharth, "A 3D Iris Scanner from a Single Image Using Convolutional Neural Networks," *IEEE Access*, vol. 8, pp. 98584–98599, 2020.

[6] K. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "Pupil dilation degrades iris biometric performance," *Computer Vision and Image Understanding*, vol. 113, no. 1, pp. 150–157, 2009.

[7] F. N. Sibai, H. I. Hosani, R. M. Naqbi, S. Dhanhani, and S. Shehhi, "Iris recognition using artificial neural networks," *Expert Systems with Applications*, vol. 38, no. 5, pp. 5940–5946, 2011.

[8] M. Tartagni and R. Guerrieri, "A fingerprint sensor based on the feedback capacitive sensing scheme," *IEEE Journal of Solid-State Circuits*, vol. 33, no. 1, pp. 133–142, 1998.

[9] F. Hidayanti, F. Rahmah, and A. Wiryawan, "Design of motorcycle security system with fingerprint sensor using arduino uno microcontroller," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 4374–4391, 2020.

[10] A. Sharma, D. Kumar, and G. Gupta, "Enhanced Iris Recognition with Histogram Cut Selection and Genetic Algorithms for Robust Classification," *Procedia Computer Science*, vol. 258, pp. 2846-2859, 2025.

[11] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it – on the (in)security of automotive remote keyless entry systems," in *Proceedings of the 25th USENIX Security Symposium*, pp. 929–944, 2016.

[12] S. Arora and M. P. S. Bhatia, "Challenges and opportunities in biometric security: A survey," *Information Security Journal*, vol. 31, no. 1, pp. 28–48, 2022, doi: 10.1080/19393555.2021.1873464.

[13] M. Faundez-Zanuy, "Biometric security technology," *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, pp. 15–26, 2006, doi: 10.1109/MAES.2006.1662038.

[14] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004, doi: 10.1109/TCSVT.2003.818349.

[15] J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993, doi: 10.1109/34.244676.

[16] S. Punnoose and J. S. J. Kumar, "Iris Recognition for Security & Safety of Automobiles," *International Journal of Innovative Science, Engineering & Technology*, vol. 2, no. 4, pp. 961–966, 2015.

[17] Z. M. Win and M. M. Sein, "Fingerprint recognition system for low quality images," in *Proceedings of the SICE Annual Conference*, vol. 2, no. 4, pp. 1133–1137, 2011.

[18] Kiruthiga Narayanasamy, "A Study of Biometric Approach for Vehicle Security System Using Fingerprint Recognition," *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, vol. 1, no. 2, pp. 10–14, 2014.

[19] K. Vishi and S. Y. Yayilgan, "Multimodal biometric authentication using fingerprint and iris recognition in identity management," in *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, pp. 334–341, 2013, doi: 10.1109/IIH-MSP.2013.91.

[20] A. Ometov and S. Bezzateev, "Multi-factor authentication: A survey and challenges in V2X applications," in *International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops*, pp. 129–136, 2017, doi: 10.1109/ICUMT.2017.8255200.

[21] G. Babu and M. Soniya, "IoT based Intelligent Car Security System using IRIS image features," *Journal of Physics: Conference Series*, vol. 1, 2021.

[22] C. Lupu and V. Lupu, "Multimodal biometrics for access control in an intelligent car," in *ISCIII'07: 3rd International Symposium on Computational Intelligence and Intelligent Informatics; Proceedings*, vol. 1, no. 2, pp. 261–267, 2007, doi: 10.1109/ISCIII.2007.367399.

[23] G. Reshma, B. T. Prasanna, H. S. N. Murthy, T. S. N. Murthy, S. Parthiban, and M. Sangeetha, "Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment," *Soft Computing*, 2023, doi: 10.1007/s00500-023-08226-5.

[24] P. J. Mehta, B. L. Parne, and S. J. Patel, "SE-LAKAF: Security enhanced lightweight authentication and key agreement framework for smart grid network," *Peer-to-Peer Networking and Applications*, vol. 16, no. 3, pp. 1513–1535, 2023, doi: 10.1007/s12083-023-01494-w.

[25] X. Duan, Y. Guo, and Y. Guo, "Design of anonymous authentication scheme for vehicle fog services using blockchain," *Wireless Networks*, vol. 30, no. 1, pp. 193–207, 2024, doi: 10.1007/s11276-023-03471-w.

[26] N. Kaliya and D. Pawar, "Unboxing fog security: a review of fog security and authentication mechanisms," *Computing*, vol. 105, no. 12, pp. 2793–2819, 2023, doi: 10.1007/s00607-023-01208-3.

[27] S. R. Borra *et al.*, "Deep hashing with multilayer CNN-based biometric authentication for identifying individuals in transportation security," *Journal of Transportation Security*, vol. 17, no. 1, 2024, doi: 10.1007/s12198-024-00272-w.

[28] T. Kaur *et al.*, "Development, detection and decipherment of obfuscated fingerprints in humans: Implications for forensic casework," *Science of Nature*, vol. 110, no. 6, 2023, doi: 10.1007/s00114-023-01886-1.

[29] D. Das, S. Banerjee, and U. Biswas, "A secure vehicle theft detection framework using Blockchain and smart contract," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 672–686, 2021, doi: 10.1007/s12083-020-01022-0.

[30] D. Das, S. Banerjee, U. Ghosh, U. Biswas, and A. K. Bashir, "A decentralized vehicle anti-theft system using Blockchain and smart contracts," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2775–2788, 2021, doi: 10.1007/s12083-021-01097-3.

[31] F. Qazi, S. A. Khan, F. Hanif, and D. E. S. Agha, "Efficient Routing Algorithm Towards the Security of Vehicular Ad-Hoc Network and Its Applications," *International Journal of Wireless Information Networks*, vol. 31, no. 1, pp. 12–28, 2024, doi: 10.1007/s10776-023-00613-x.

[32] M. A. Akram, A. N. Mian, and S. Kumari, "Fog-based low latency and lightweight authentication protocol for vehicular communication," *Peer-to-Peer Networking and Applications*, vol. 16, no. 2, pp. 629–643, 2023, doi: 10.1007/s12083-022-01425-1.

[33] S. Shomaji, Z. Guo, F. Ganji, N. Karimian, D. Woodard, and D. Forte, "BLOcKeR: A Biometric Locking Paradigm for IoT and the Connected Person," *Journal of Hardware and Systems Security*, vol. 5, no. 3–4, pp. 223–236, 2021, doi: 10.1007/s41635-021-00121-5.

[34] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," *International Journal on Interactive Design and Manufacturing*, vol. 15, no. 2–3, pp. 365–380, 2021, doi: 10.1007/s12008-021-00760-6.

[35] R. Sujarani, D. Manivannan, R. Manikandan, and B. Vidhyacharan, "Lightweight Bio-Chaos Crypt to Enhance the Security of Biometric Images in Internet of Things Applications," *Wireless Personal Communications*, vol. 119, no. 3, pp. 2517–2537, 2021, doi: 10.1007/s11277-021-08342-1.

[36] A. Goswami, S. Rana, and D. Chhikara, "An efficient blockchain assisted dynamic authentication scheme for geo-spatial enabled vehicular network," *Telecommunication Systems*, vol. 83, no. 3, pp. 241–251, 2023, doi: 10.1007/s11235-023-01016-2.

[37] R. Shikka, R. Kamalraj, P. K. Shah, K. Sutariya, S. R. Anwar, and A. Kumar, "Intelligent algorithms in privacy-preserving authentication schemes and traceability with accuracy in VANETs for smart transportation," *Soft Computing*, vol. 28, no. 23, pp. 13853–13862, 2024, doi: 10.1007/s00500-023-08634-7.

[38] G. Kumar and A. Altalbe, "Artificial intelligence (AI) advancements for transportation security: in-depth insights into electric and aerial vehicle systems," *Environment, Development and Sustainability*, 2024, doi: 10.1007/s10668-024-04790-4.

[39] S. A. Sivasankari, D. Gupta, I. Keshta, C. V. K. Reddy, P. P. Singh, and H. Byeon, "Anonymity and security improvements in heterogeneous connected vehicle networks," *International Journal of Data Science and Analytics*, vol. 19, no. 4, pp. 749–762, 2025, doi: 10.1007/s41060-023-00499-1.

[40] K. Bayoudh, R. Knani, F. Hamdaoui, and A. Mtibaa, "A survey on deep multimodal learning for computer vision: advances, trends, applications, and datasets," *Visual Computer*, vol. 38, no. 8, pp. 2939–2970, 2022, doi: 10.1007/s00371-021-02166-7.

[41] S. M. Taylor and M. De Leeuw, "Guidance systems: from autonomous directives to legal sensor-bilities," *AI and Society*, vol. 36, no. 2, pp. 521–534, 2021, doi: 10.1007/s00146-020-01012-z.

[42] S. Quach, P. Thaichon, K. D. Martin, S. Weaven, and R. W. Palmatier, "Digital technologies: tensions in privacy and data," *Journal of the Academy of Marketing Science*, vol. 50, no. 6, pp. 1299–1323, 2022, doi: 10.1007/s11747-022-00845-y.

[43] M. Xiao, L. Chen, H. Feng, Z. Peng, and Q. Long, "Smart City Public Transportation Route Planning Based on Multi-objective Optimization: A Review," *Archives of Computational Methods in Engineering*, vol. 31, no. 6, pp. 3351–3375, 2024, doi: 10.1007/s11831-024-10076-9.

[44] V. L. Raposo, "The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal," *European Journal on Criminal Policy and Research*, vol. 29, no. 4, pp. 515–533, 2023, doi: 10.1007/s10610-022-09512-y.

[45] M. Khare, A. Khare, M. Jeon, and I. K. Sethi, "Machine vision theory and applications for cyber-physical systems," *Multimedia Tools and Applications*, vol. 81, no. 16, pp. 21995–22000, 2022, doi: 10.1007/s11042-022-13261-9.

[46] Arshi and Mondal, "Smart Construction and Sustainable Cities Advancements in sensors and actuators technologies for smart cities: a comprehensive review," *Smart Construction and Sustainable Cities*, vol. 1, no. 18, 2023.

[47] L. Yang *et al.*, "Exploring the role of computer vision in product design and development: a comprehensive review," *International Journal on Interactive Design and Manufacturing*, vol. 18, no. 6, pp. 3633–3680, 2024, doi: 10.1007/s12008-024-01765-7.

[48] V. Rao and K. V. Prema, "A review on lightweight cryptography for Internet-of-Things based applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 8835–8857, 2021, doi: 10.1007/s12652-020-02672-x.

[49] L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "BACTmobile: A Smart Blood Alcohol Concentration Tracking Mechanism for Smart Vehicles in Healthcare CPS Framework," *SN Computer Science*, vol. 3, no. 3, 2022, doi: 10.1007/s42979-022-01142-9.

[50] C. B. Tan *et al.*, "A survey on presentation attack detection for automatic speaker verification systems: State-of-the-art, taxonomy, issues and future direction," *Multimedia Tools and Applications*, vol. 80, no. 21–23, pp. 32725–32762, 2021, doi: 10.1007/s11042-021-11235-x.

[51] R. De Smet, T. Vandervelden, K. Steenhaut, and A. Braeken, "Lightweight PUF based authentication scheme for fog architecture," *Wireless Networks*, vol. 27, no. 2, pp. 947–959, 2021, doi: 10.1007/s11276-020-02491-0.

[52] S. Rana, D. Mishra, C. Lal, and M. Conti, "Authenticated Message-Exchange Protocol for Fog-Assisted Vehicular Cloud Computing," *Wireless Personal Communications*, vol. 131, no. 2, pp. 1295–1312, 2023, doi: 10.1007/s11277-023-10480-7.

[53] H. S. Grover, Adarsh, and D. Kumar, "Cryptanalysis and improvement of a three-factor user authentication scheme for smart grid environment," *Journal of Reliable Intelligent Environments*, vol. 6, pp. 249–260, 2020.

[54] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 21, no. 1, pp. 115–158, 2022, doi: 10.1007/s10207-021-00545-8.

[55] A. Alagumalai *et al.*, "Self-powered sensing systems with learning capability," *Joule*, vol. 6, no. 7, pp. 1475–1500, 2022, doi: 10.1016/j.joule.2022.06.001.

[56] A. K. Tyagi and S. U. Aswathy, "Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future," *International Journal of Intelligent Networks*, vol. 2, pp. 83–102, 2021, doi: 10.1016/j.ijin.2021.07.002.

[57] P. Y. Tseng, P. C. Lin, and E. Kristianto, "Vehicle theft detection by generative adversarial networks on driving behavior," *Engineering Applications of Artificial Intelligence*, vol. 117, 2023, doi: 10.1016/j.engappai.2022.105571.

[58] Z. Chen, X. Feng, and S. Zhang, "Emotion detection and face recognition of drivers in autonomous vehicles in IoT platform," *Image and Vision Computing*, vol. 128, 2022, doi: 10.1016/j.imavis.2022.104569.

[59] S. T. Banafshehvaragh and A. M. Rahmani, "Intrusion, anomaly, and attack detection in smart vehicles," *Microprocessors and Microsystems*, vol. 96, 2023, doi: 10.1016/j.micpro.2022.104726.

[60] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, 2024, doi: 10.1016/j.iotcps.2023.12.003.

[61] B. D. Deebak, "Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems," *Sustainable Cities and Society*, vol. 63, 2020, doi: 10.1016/j.scs.2020.102416.

[62] M. H. Khan, A. R. Javed, Z. Iqbal, M. Asim, and A. I. Awad, "DivaCAN: Detecting in-vehicle intrusion attacks on a controller area network using ensemble learning," *Computers and Security*, vol. 139, pp. 947–959, 2024, doi: 10.1016/j.cose.2024.103712.

[63] R. Casanova-Marqués, J. Torres-Sospedra, J. Hajny, and M. Gould, "Maximizing privacy and security of collaborative indoor positioning using zero-knowledge proofs," *Internet of Things (Netherlands)*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100801.

[64] G. Sabaliauskaite, J. Bryans, H. Jadidbonab, F. Ahmad, S. Shaikh, and P. Wooderson, "TOMSAC - Methodology for trade-off management between automotive safety and cyber security," *Computers and Security*, vol. 140, 2024, doi: 10.1016/j.cose.2024.103798.

[65] Y. Guo and Y. Guo, "FogHA: An efficient handover authentication for mobile devices in fog computing," *Computers and Security*, vol. 108, 2021, doi: 10.1016/j.cose.2021.102358.

[66] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, p. 100411, 2021, doi: 10.1016/j.cosrev.2021.100411.

[67] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *Journal of Network and Computer Applications*, vol. 204, 2022, doi: 10.1016/j.jnca.2022.103414.

[68] F. Ghaffari, E. Bertin, N. Crespi, and J. Hatin, "Distributed ledger technologies for authentication and access control in networking applications: A comprehensive survey," *Computer Science Review*, vol. 50, 2023, doi: 10.1016/j.cosrev.2023.100590.

[69] D. Dharminder, U. Kumar, and P. Gupta, "Edge based authentication protocol for vehicular communications without trusted party communication," *Journal of Systems Architecture*, vol. 119, 2021, doi: 10.1016/j.sysarc.2021.102242.

[70] M. S. Almadani, S. Alotaibi, H. Alsobhi, and O. K. Hussain, "Blockchain-based multi-factor authentication: A systematic literature review," *Internet of Things*, vol. 23, 2023.

[71] J. W. Lee, W. K. Lee, and S. Y. Sohn, "Patenting trends in biometric technology of the Big Five patent offices," *World Patent Information*, vol. 65, 2021, doi: 10.1016/j.wpi.2021.102040.

[72] Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, M. M. Kabir, and M. F. Mridha, "Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review," *Computers and Security*, vol. 140, 2024, doi: 10.1016/j.cose.2024.103747.

[73] H. Yang, Y. Guo, and Y. Guo, "Blockchain-based cloud-fog collaborative smart home authentication scheme," *Computer Networks*, vol. 242, 2024, doi: 10.1016/j.comnet.2024.110240.

[74] Z. Wang, D. Deng, S. Hou, Y. Guo, and S. Li, "Design of three-factor secure and efficient authentication and key-sharing protocol for IoT devices," *Computer Communications*, vol. 203, pp. 1–14, 2023, doi: 10.1016/j.comcom.2023.02.015.

[75] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things Security–A review," *Cyber Security and Applications*, vol. 3, 2025, doi: 10.1016/j.csa.2024.100057.

[76] P. Srinivasan, S. Anthoniraj, K. Anguraj, S. Kumarganesh, and B. Thiyaneswaran, "Development of keyless biometric authenticated vehicles ignition system," *Materials Today: Proceedings*, vol. 81, no. 2, pp. 464–469, 2021, doi: 10.1016/j.matpr.2021.03.632.

[77] B. Khalid, K. N. Qureshi, K. Z. Ghafoor, and G. Jeon, "An improved biometric based user authentication and key agreement scheme for intelligent sensor based wireless communication," *Microprocessors and Microsystems*, vol. 96, 2023, doi: 10.1016/j.micpro.2022.104722.

[78] E. Haodudin Nurkifli and T. Hwang, "Provably secure authentication for the internet of vehicles," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 8, 2023, doi: 10.1016/j.jksuci.2023.101721.

[79] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *Journal of Information Security and Applications*, vol. 82, 2024, doi: 10.1016/j.jisa.2024.103748.

[80] V. Kumar, "RSFVC: Robust Biometric-Based Secure Framework for Vehicular Cloud Networking," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 5, pp. 3364–3374, 2024, doi: 10.1109/TITS.2023.3322960.

[81] M. Tanveer, A. U. Khan, H. Shah, S. A. Chaudhry, and A. Naushad, "PASKE-IoD: Privacy-Protecting Authenticated Key Establishment for Internet of Drones," *IEEE Access*, vol. 9, pp. 145683–145698, 2021, doi: 10.1109/ACCESS.2021.3123142.