ABSTRACT

The historical evolution of transportation has witnessed remarkable advancements, from the invention of the wheel to the era of steam-powered locomotives and automobiles. Each phase has been marked by innovations reshaping how we navigate our surroundings. In contemporary times, the amalgamation of cutting-edge technologies has given rise to a new epoch in transportation with the advent of Connected and Autonomous Vehicles (CAVs). This evolution is spurred by the pressing need for safer, more efficient, and sustainable transportation solutions. As urbanization intensifies, challenges related to traffic congestion, vehicular accidents, and environmental impacts become increasingly pronounced. In response, researchers and engineers have sought innovative ways to leverage technology and connectivity, giving rise to the concept of autonomous vehicles.

CAVs, equipped with sophisticated sensors, artificial intelligence, and communication technologies, embody a revolutionary leap forward in transportation. They hold the promise of redefining the driving experience by automating critical functions, reducing human error, and optimizing traffic flow. The incorporation of connectivity, allowing vehicles to communicate with each other (V2V) and with infrastructure (V2I), further enhances their potential impact on road safety and efficiency. However, this interconnectedness brings forth new challenges, particularly concerning the privacy of personal data collected within the CAV network.

The proliferation of sensors and communication capabilities in CAVs raises significant privacy concerns. As these vehicles generate and exchange vast amounts of data, ranging from location information to personal preferences, ensuring the privacy and security of individuals becomes paramount. Concerns arise regarding unauthorized access to sensitive data, the potential for data breaches, and the risk of malicious exploitation. The need for a robust framework that safeguards both the security and privacy of users within the CAV ecosystem is essential for fostering public trust and widespread adoption.

In response to these privacy challenges, researchers and technologists have turned to blockchain technology as a potential solution. Blockchain's inherent characteristics, including decentralization, transparency, and cryptographic

security, position it as a promising tool to address privacy concerns in the context of CAVs. The integration of blockchain technology can provide a tamper-resistant and secure platform for the storage and exchange of sensitive data, ensuring the confidentiality of personal information. This becomes especially crucial as CAVs operate in an environment where data integrity and user privacy are central to building public acceptance and trust in autonomous transportation.

As CAVs continue to evolve, the need for a systematic approach to enhancing both security and privacy becomes imperative. Multi-Criteria Decision Making (MCDM) techniques, such as Fuzzy TOPSIS and Fuzzy AHP, emerge as essential tools to guide decision-making processes in selecting suitable blockchain frameworks. These methodologies contribute to the systematic evaluation of blockchain alternatives, considering factors such as scalability, latency, and security features. The integration of blockchain and MCDM techniques not only fortifies the security infrastructure of CAVs but also addresses the nuanced privacy concerns that arise in the interconnected and data-rich environment of autonomous vehicles.

The research methodology undertaken in this thesis unfolds across five distinct and interrelated phases, each contributing to the overarching goal of enhancing the security infrastructure of Connected and Autonomous Vehicles (CAVs). The initial phase, the Identification Phase, is a critical starting point, involving an exhaustive examination of security parameters intrinsic to CAVs. This includes the identification of sub-parameters and an extensive review of existing alternatives, particularly blockchain frameworks, which serve as the bedrock for securing CAVs in the dynamically evolving transportation landscape.

Following the Identification Phase, the Categorization Phase takes center stage, where the identified parameters and sub-parameters are meticulously mapped, elucidating the intricate relationships between these elements. This structured categorization provides a visual framework, offering insights into the nuanced connections within the security landscape of CAVs. The clarity achieved in this phase sets the stage for more informed decision-making in subsequent stages.

The Computation Phase is where the methodology integrates advanced decision-making techniques. Fuzzy Analytic Hierarchy Process (Fuzzy AHP) is employed to systematically assess and rank the identified parameters and sub-parameters based on their influence on CAV security. Simultaneously, Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy TOPSIS) is deployed to pinpoint the most optimal blockchain alternative among the identified options. This computational layer not only introduces a quantitative dimension to the decision-making process but also ensures a comprehensive evaluation of potential solutions.

Transitioning from theory to practical implementation, the Designing Phase utilizes the insights gained from the preceding phases to develop a privacy-preserving model. This model is custom-tailored for CAVs and leverages the optimal blockchain framework identified in earlier stages. The Designing Phase marks the tangible application of the theoretical constructs, offering a real-world solution for enhancing privacy and security within the CAV ecosystem.

The Validation Phase serves as the concluding segment, subjecting the proposed solution to rigorous scrutiny. Sensitivity analysis is conducted to assess the stability of outcomes derived from Fuzzy AHP and Fuzzy TOPSIS, offering insights into the reliability of the proposed methodology. Comparative evaluations with other Multi Criteria Decision Making techniques further validate the robustness of the proposed security enhancements. Statistical analyses, incorporating both null and alternative hypotheses, provide a comprehensive empirical validation, ensuring the proposed methodology aligns with established benchmarks.

In conclusion, this research represents a significant step forward in fortifying the security of Connected and Autonomous Vehicles (CAVs). The systematic methodology employed in this study, encompassing the identification of security parameters, categorization of relationships, computational analysis, designing of a privacy-preserving model, and rigorous validation, contributes a comprehensive framework for enhancing CAV security.

The derived benefits from this research are multifaceted. The methodology offers stakeholders a systematic and informed approach to selecting blockchain

frameworks, fostering a more secure and trustworthy CAV ecosystem. The privacy-preserving model, grounded in theoretical constructs, offers practical applications that enhance real-world security and privacy for CAVs. The empirical validation conducted ensures the reliability and effectiveness of the proposed methodology, instilling confidence in its applicability.

Looking forward, the future scope of this research is expansive. Continual refinement and adaptation of the proposed model to address emerging security challenges and advancements in technology are imperative. Expanding the scope of security considerations, addressing scalability issues associated with blockchain, and exploring solutions for seamless integration within large-scale CAV networks present critical avenues for future research. As technology evolves, this work establishes a foundation for ongoing advancements in security measures for CAVs, contributing to a resilient and secure future for connected and autonomous transportation.