ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 9, Issue 4, 2021

Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges

Sreekar Peddi
Tek Leaders, Plano, Texas, USA
Email ID: sreekarpeddi95@gmail.com

ABSTRACT
Vehicular Cloud Computing (VCC) is a paradigm-shifting approach that combines cloud computing and vehicular networks to provide improved services and increased system efficiency in transportation. However, because of its complexity and dynamic nature, VCC presents serious security and privacy challenges. This study focuses on finding vulnerabilities and recommending strong security measures by doing a thorough analysis of threat models in VCC. To improve secure collaboration among vehicles, it presents a trust-based method known as Double Board-based Trust Estimation and Correction, or DBTEC. In addition to a dynamic collaboration route building method, DBTEC combines direct trust estimation through a Private board and indirect trust estimation through a Public board. This approach adjusts to the changing VCC environment and enhances the identification of trustworthy cooperation partners. The study validates the effectiveness of DBTEC in boosting cooperation rates and guaranteeing security through comprehensive theoretical analysis and simulations. A review of the literature places the importance of addressing security in VCC in perspective and draws attention to research gaps that currently exist. From a methodological standpoint, the study makes use of threat modeling methodologies like CIAA and STRIDE to systematically identify and evaluate possible dangers. This research seeks to improve the integrity and dependability of VCC systems by putting forth and validating a complete security architecture. This will further the field of vehicular cloud computing and promote safer and more effective vehicular networks.

Keywords: Vehicular Cloud Computing (VCC), Threat Modeling, DBTEC, Trust-Based Approach, STRIDE, CIAA, Intrusion Detection Systems, Access Control Mechanisms, System Performance, Mitigation Effectiveness.

1. INTRODUCTION

Investigating the complex field of Vehicular Cloud Computing (VCC), the study focuses on threat model analysis and the ensuing security and privacy issues. Vehicle-cloud computing, or VCC, is a new and exciting paradigm with wide-ranging effects on transportation systems. But there are a lot of security and privacy issues raised by this confluence, so careful consideration is required. The study intends to provide strong security measures and privacy safeguards to guarantee the integrity and confidentiality of vehicle cloud computing environments by examining threat models within the VCC framework and highlighting vulnerabilities and potential hazards.

ISSN2321-2152
www.ijmece .com
Vol 9, Issue 4, 2021

Background: Vehicular Cloud Computing (VCC) has emerged as a result of the growing integration of cloud computing with vehicular networks. VCC allows vehicles to operate together and offer a range of services, including package delivery. However, the existence of bad actors presents serious obstacles to the security cooperation of cars in the VCC. This article suggests a trust-based approach called DBTEC to improve security collaboration in VCC as a response. To calculate trust values for choosing cooperative partners, the DBTEC scheme makes use of both direct trust estimate through a Private board and indirect trust estimation through a Public board. It also presents a dynamic cooperation route creation strategy to build cooperation paths and choose cooperative cars in an adaptive manner. Extensive theoretical analysis and simulation are used to show the efficacy of the proposed paradigm, showing benefits in security and reliability in VCC settings. By tackling the important security and privacy issues in VCC, this research eventually improves the reliability and effectiveness of vehicular cloud computing systems.

Purpose: This study explores the field of Vehicular Cloud Computing (VCC), in which automobiles work together to carry out different tasks, such package delivery, while having to contend with threats from outside sources. In order to promote safe cooperation amongst cars in VCC, the article suggests a trust-based approach called DBTEC. As opposed to traditional methods, DBTEC calculates the possible cooperative partners' trustworthiness by combining direct trust estimation from a Private board and indirect trust estimation from a Public board. Furthermore, a dynamic collaboration path creation technique is presented to improve work success and safety. The efficiency of the suggested paradigm in raising collaboration completion rates and guaranteeing security is proven through in-depth theoretical research and simulations. The dependability and integrity of automotive cloud computing environments are improved by this research's contribution to resolving the urgent security issues in VCC.

Objective: In this research work, a trust-based architecture called DBTEC is proposed as a solution to security collaboration issues in Vehicular Cloud Computing (VCC). Due to the existence of hostile entities, vehicles that use the collaborative computing paradigm (VCC) face major security challenges. The DBTEC approach evaluates cooperative partners' trustworthiness by combining direct trust estimation from a Private board and indirect trust estimation from a Public board. A dynamic collaboration path construction approach is also presented to improve task completion rates. Improvements in trustworthiness evaluation, higher cooperation completion rates, and improved security collaboration in VCC are the paper's main goals. It is shown that the suggested DBTEC paradigm is effective in terms of security and reliability through theoretical analysis and simulation. The knowledge and application of safe cooperation methods in vehicular cloud computing systems are advanced by this paper.

Research Gap: A significant research vacuum in Vehicular Cloud Computing (VCC) is filled by the suggested trust-based paradigm, dubbed DBTEC, which offers a methodical approach to security collaboration in the face of malevolent vehicles. DBTEC integrates both direct trust

estimate from private interactions and indirect trust estimation from a public board, in contrast to prior systems that only use direct interactions for trust estimation. This novel method improves the identification of reliable working partners and enriches the trust evaluation procedure. In addition, the study presents a dynamic cooperation path creation technique that addresses the static nature of conventional approaches and adjusts to the changing VCC environment. The usefulness of the DBTEC scheme in improving security and reliability inside VCC is shown through thorough theoretical analysis and simulation, addressing a key research gap.

Problem Statement: The challenge of guaranteeing safe cooperation between vehicles in Vehicular Cloud Computing (VCC) settings is the focus of this research article, especially in situations when numerous vehicles must collaborate to complete a job. The two main problems are the inability to identify reliable cooperation partners due to the lack of trust information among vehicles and the necessity of ensuring task success and safety, particularly when physical goods are involved. The research suggests a novel trust-based approach for fostering secure cooperation in VCC termed DBTEC (Double Board based Trust Estimation and Correction) in order to address these issues. This paradigm allows for the more efficient selection of cooperative partners and the dynamic development of cooperative paths by integrating both indirect trust estimation from a public board and direct trust estimation from private interactions. The suggested method allows cars to make judgments based on thorough trust information, which improves security and dependability in VCC circumstances.

2. LITERATURE SURVEY

Kashevnik et al. (2020) investigate the application of smartphone sensors to identify a range of possible hazards in car interiors, including fatigue, distraction, and reckless actions. Their study explores the complex information flow between drivers, cars, and intelligent transportation systems (ITS), analyzing potential weak points that might appear. Through an analysis of the dynamics of situation monitoring during vehicle control and ITS interaction, the article clarifies the main information flows and the risks that accompany them. It also classifies threat classes that are relevant to controlling a vehicle and evaluates the likelihood that these threats will be picked up by smartphone sensors. These results are supported by an engaging case study that illustrates how smartphone sensors may reliably detect risks like fatigue, attention, loose seatbelts, and eating, drinking, and using a smartphone while driving.

Bakhshi Valojerdi and Balador (2019) investigate the field of fog computing, a rapidly developing paradigm that brings cloud services to the edge of networks and provides dynamic mobility assistance and low-latency communication—perfect for applications in cars. This invention does, however, come with some security and privacy risks, making fog computing open to possible attacks from unidentified enemies. The study provides light on the complex interactions between security, privacy, and the development of safety-critical applications by carefully reviewing current flaws and remedies relevant to fog-based vehicular networks. It also maps out open

difficulties and future research possibilities in this emerging subject, opening the door for improved privacy and security protocols in fog computing settings.

In a new research work, Shao et al. (2018) present a dynamic data integrity auditing method designed for the automotive cloud. The suggested plan aims to address common problems with current integrity auditing techniques, such as ineffectiveness, vulnerabilities related to data privacy, and high expenses. Using bilinear pairing mapping technology in conjunction with a hierarchical multiple branches tree data authentication structure, the technique guarantees auditing accuracy and strengthens resilience against possible attacks. The study's performance analysis shows improved time efficiency over traditional techniques, indicating the scheme's feasibility in resolving important issues and improving the integrity auditing landscape in vehicle cloud environments.

The complexity of security issues in automotive networks is explored by Hoque and Hasan (2019), who highlight the need for a strong threat model designed for automotive fog computing. The authors propose that, in light of the changing environment, it is beneficial to utilize STRIDE and CIAA threat modeling techniques in order to methodically recognize the risks and weaknesses present in this computing paradigm. They claim that by using this strategy, the security and privacy of car fog computing systems may be greatly enhanced, overcoming the particular difficulties brought on by the enormous size, high mobility, and dynamic topology of car networks. In order to fully comprehend and mitigate security threats, this study emphasizes how crucial threat modeling is. This will help to maintain the integrity of vehicular fog computing ecosystems and promote resilience.

Masood et al. (2020) investigate the field of vehicular cloud computing (VCC), which is a development of standard cloud computing that is designed to make resource sharing and problem-solving between vehicles easier. As a result of its unique features, which include multitenancy, sporadic wireless connectivity, high mobility, and decentralized operation, VCC faces significant security and privacy challenges despite its potential. In this paper, VCC is thoroughly examined, with an emphasis on its architecture, unique characteristics, and range of applications. In addition, it carefully examines a range of possible risks and privacy issues that are inherent to VCC, setting the stage for next studies that will strengthen its security and expand its capabilities.

Malamer et al. (2018) explore the field of connected vehicular cloud computing (CVCC), a new paradigm that utilizes the combined power of networked cars. This study examines the security risks associated with CVCC and suggests a new game-theoretic framework designed to encourage car owners to increase their security precautions, strengthening the system's overall resilience. The study also presents a thorough architecture for CVCC, clarifies its various uses, and thoroughly investigates a range of security concerns and incentive systems. Using a two-phase heterogeneous public good game model, the research investigates how different incentive schemes and network configurations affect vehicle owners' investment choices within the CVCC ecosystem.

In the field of Vehicular Cloud Computing (VCC), Xue et al. (2018) introduce a novel fog-to-cloud architecture designed for safe data exchange. Recognizing how crucial it is to protect privacy and implement strong security measures in VCC, the study introduces a novel plan to handle the inherent difficulties. To reduce response time and reduce processing overhead, this architecture makes use of cryptography and fine-grained access control techniques. Notably, the suggested approach ensures accountability and transparency by enabling verifiable auditing of the reports generated by fog servers. The study highlights the effectiveness and practicality of the developed method by presenting significant improvements in response time and overhead reduction through extensive experimental testing.

According to Onwubiko (2017), there is a growing discrepancy between cybersecurity measures and the changing nature of cyber-threats. This means that security operations centers (SOCs) need to be implemented with resilience in order to continuously monitor and detect potential exploits. The study highlights the dynamic trajectory of cybersecurity developments in the context of the swiftly evolving technology, exposing a clear disparity between the sophistication of cyberthreats and the effectiveness of current security measures. This imbalance is made worse by the lack of properly formed SOCs, which leaves firms more susceptible to new attacks. The study recommends deployment strategies that strengthen defenses against both conventional and advanced vulnerabilities and improve situational awareness in order to promote a more robust cybersecurity posture.

Aladwan et al. (2019) investigate the vital importance of security in Internet of Things (IoT)-powered smart cities, with a special emphasis on the domains of cloud-based vehicular clouds and the internet of vehicles (IoV). The research has a difficult task in accurately calculating and evaluating security levels amidst the increasing complexity of these paradigms. The study uses a context-based analysis to identify common security requirements that are necessary to protect these complex systems. Furthermore, in order to maintain data secrecy, the study presents a novel privacy granularity classification system, providing an organized framework that can help choose strong security solutions.

Mishra et al. (2020) explore the emerging field of vehicle networking, highlighting its critical function in improving road safety, traffic control, and information distribution. Acknowledging the revolutionary possibilities of vehicular cloud computing (VCC), the study presents a novel architecture that enhances communication effectiveness by utilizing cloud computing infrastructure, IoT environment, and vehicular resources. In light of the urgent requirement for strong mutual authentication schemes in VCC, the paper presents a new approach based on chaotic maps. This framework solves authentication issues that arise with VCC systems in addition to guaranteeing the safe and effective interchange of data. The research provides concrete evidence of the communication and computing efficiency of the suggested scheme in comparison to current

paradigms by utilizing simulation tools and thorough security analysis to validate its effectiveness and superiority.

In order to assure collision prevention in linked environments, Sheik et al. (2017) tackle the crucial issue of data computation location for Collaborative Cruise Control (CCC). They do this by delving into the complexities of integrating Adaptive Cruise Control (ACC) inside a collaborative ecosystem. The study emphasizes how important it is for system efficacy for the Internet of Things (IoT) and Intelligent Transportation Systems (ITS) to work together, acknowledging their mutually beneficial relationship. In the face of the difficulty of incorporating ACC into cooperative environments, the study emphasizes how critical it is to use safe and dependable Cruise Control (CC) in order to achieve complete vehicle autonomy, especially when using the Cloud and Edge Cloud frameworks. The work paves the way for safer and more effective connected environments by developing an application model and taxonomy that provide an organized method for determining the best position for computational data in CCC.

3. METHODOLOGY

The current work takes a thorough and comprehensive approach to investigating threat models linked to vehicular cloud computing (VCC), with an emphasis on security and privacy concerns. The study technique consists of numerous exhaustive steps, beginning with a thorough review of the existing literature. These are followed by a thorough threat modeling approach, accurate vulnerability detection, and the creation of strong security solutions. To provide a comprehensive overview of the research technique, each phase is explained below:

3.1. Literature Review

The first step in the research is to read the extensive body of literature that has already been written about Vehicular Cloud Computing (VCC), security protocols, privacy issues, and threat modeling techniques. This preliminary step involves reading a wide range of scholarly articles, conference papers, technical reports, and industrial publications in order to obtain crucial information on the topic's current state. Following a comprehensive review of the literature, the study seeks to highlight significant concerns pertaining to VCC settings, identify knowledge gaps, and pinpoint recurrent patterns.

3.2. Threat Modeling

The research builds on the core insights gleaned from the comprehensive literature evaluation to start the crucial step of developing a comprehensive threat model that is particularly suited to the intricacies of vehicular cloud computing (VCC). An important step that marks a significant advancement in the study's methodology is the methodical identification and classification of potential dangers and attack vectors that vehicles and cloud infrastructure may encounter inside the dynamic landscape of VCC scenarios.

In the context of VCC, threat modeling is a multimodal approach that includes well-known methods such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege) and CIAA (Confidentiality, Integrity, Availability, Accountability). Stakeholders can more easily understand the security and privacy concerns they

ISSN2321-2152

www.ijmece .com

Vol 9, Issue 4, 2021

must address since these frameworks provide an orderly way to analyze and dissect the many risks inherent to VCC.

$$R_{VCC}=\sum_{i=1}^{n}(D_i \times A_i) \quad (1)$$

Where:

RVCC - represents the total risk in vehicular cloud computing (VCC).

- indicates the intensity of each identified threat or attack vector.
- reflects the chance of encountering each risk or assault vector.

This equation calculates the total risk in VCC by summing the severity level and probability products for each indicated hazard or attack vector.

The initial stage in the threat modeling process is identifying potential threat actors or other entities that could jeopardize the security and integrity of VCC environments. Threat actors encompass a diverse range of adversaries, including malicious individuals, cybercriminals, and even rogue vehicles that seek to exploit vulnerabilities in the system to their own gain. By identifying the various threat actors and their motivations, the research lays the groundwork for the development of specialized security solutions meant to lessen specific threats.

The threat actors are listed first, followed by a list of all potential attack vectors and tactics that these adversaries might employ to compromise the security of VCC systems. These attack vectors encompass an extensive spectrum of tactics, ranging from intricate techniques such as GPS spoofing and man-in-the-middle attacks to more traditional approaches like malware infiltration and data breaches. Through a meticulous cataloging of numerous attack routes, the research aims to provide a comprehensive understanding of the potential vulnerabilities in VCC environments and design effective remedies to mitigate these risks.

The study begins by enumerating the attack vectors and then assesses the potential impact of these threats on the four primary components of VCC security: confidentiality, integrity, availability, and accountability. Through a thorough analysis informed by the CIAA paradigm, the study evaluates the potential repercussions of security breaches and privacy violations inside VCC environments, taking into account the wider implications for stakeholders like as cloud service providers, end users, and vehicle operators.

The research also attempts to quantify the likelihood of various threat scenarios occurring in VCC situations by taking into consideration factors such as system architecture, network topology, and threat actor capabilities. The Fig 1 employs risk assessment approaches and probabilistic models to rate security threats based on potential impact and likelihood, thereby assisting stakeholders in more effective resource allocation and mitigation measures.

ISSN2321-2152
www.ijmece .com
Vol 9, Issue 4, 2021

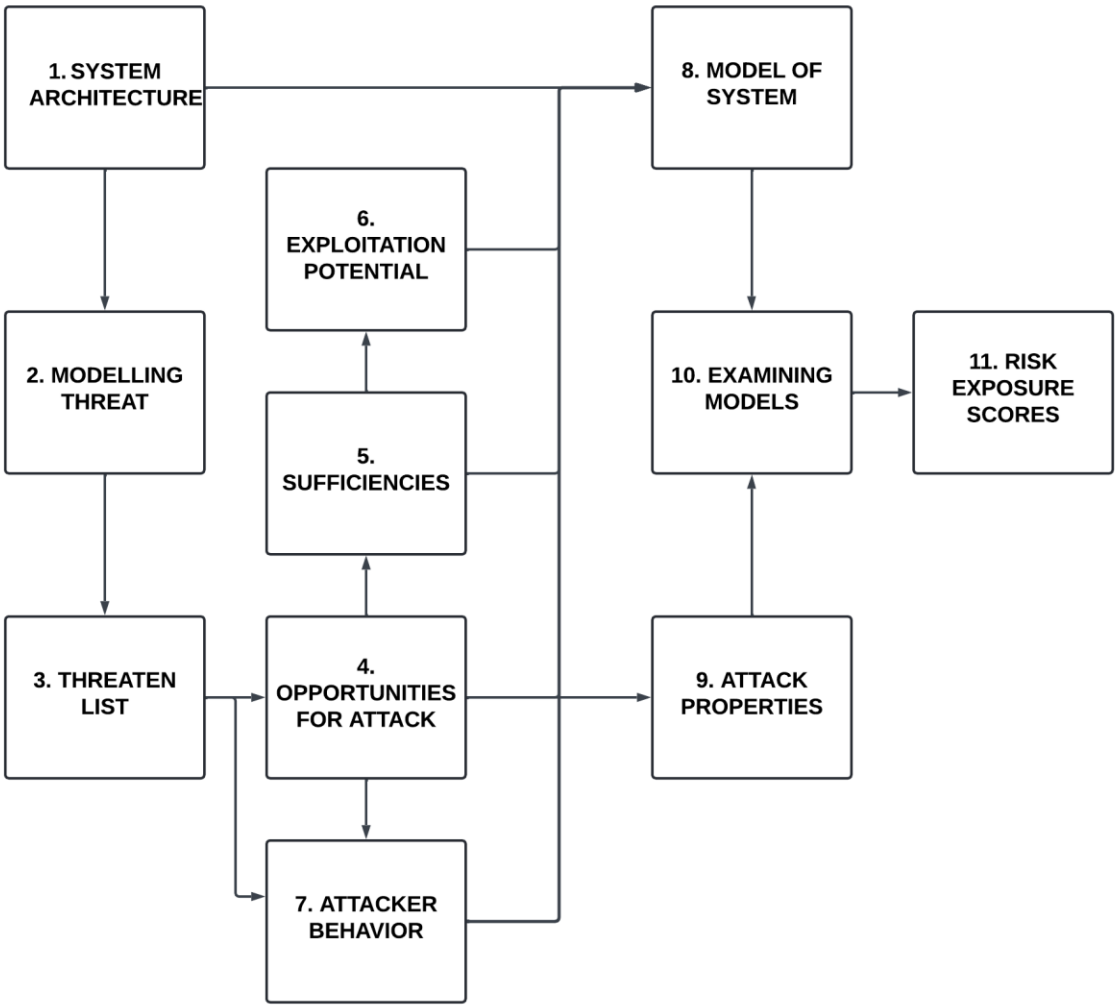

Figure 1: Threat modeling and formal methodology are used to conduct risk analysis.

In addition to assessing the likelihood and implications of security concerns, the study looks into the viability of potential mitigation and countermeasure strategies aimed at these dangers. The effectiveness of various security controls, including access control mechanisms, encryption techniques, and intrusion detection systems, in reducing specific threats in VCC environments is evaluated in this study. It accomplishes this by utilizing knowledge gleaned from the literature study and threat analysis. The research also takes into account the potential disadvantages and trade-offs of implementing certain security measures, taking into account factors like cost, complexity, and scalability.

The threat modeling approach is often considered the main tenet of the study methodology since it provides a systematic framework for identifying, assessing, and mitigating security and privacy vulnerabilities in systems that use vehicular cloud computing. CIAA and STRIDE are two well-

ISSN2321-2152
www.ijmece .com
Vol 9, Issue 4, 2021

known techniques that will be used in this study to strengthen the security posture of VCC systems and decrease the effect of any risks on stakeholders and end users.

Table 1: Threat Actors, Attack Vectors, Impact, and Mitigation Strategies in Vehicular Cloud Computing (VCC).

Threat actors	Potential attack vectors	Effect on Security at VCC	Strategies for Mitigation
Malicious Individuals	Man-in-the-Middle Attacks and GPS Spoofing	High	Intrusion Detection Systems and encryption
Cybercriminals	Infiltration of Malware and Data Breach	High	Mechanisms for Access Control and Encryption
Rogue Vehicles	Data manipulation and unauthorized access	Medium	Secure Communication Protocols and Authentication Mechanisms

Potential threat actors, attack vectors, and their effects on VCC security are shown in Table 1. Through GPS spoofing and man-in-the-middle assaults, malicious persons pose a high danger that is reduced by intrusion detection and encryption. Through malware and data breaches, cybercriminals pose a high risk that can be mitigated by access control and encryption. Data modification by rogue cars is a medium danger, which is mitigated by secure communication protocols and authentication systems.

3.3. Identification of Vulnerabilities

The research now focuses on the meticulously detailed identification of vulnerabilities woven throughout the architecture of Vehicle Cloud Computing systems, with the threat model firmly in place. This significant study includes a thorough examination of the various components that comprise virtual cloud computing ecosystems, such as vehicle networks, data storage systems, cloud computing infrastructure, and communication protocols. Using meticulous inspection, common vulnerabilities such as inadequate access controls, shoddy authentication techniques, and unsecured communication channels are methodically identified, noted, and categorized.

3.4. Proposing Security Solutions

The research seeks to create robust security solutions that lower risks and improve the security posture of VCC systems by utilizing a thorough understanding of the threats and vulnerabilities found. The study proposes to develop a strong security framework that can address the unique challenges posed by virtual computer environments by utilizing a wide range of security measures, including intrusion detection systems, access control mechanisms, cryptography, and secure communication protocols. The major goal is to develop security solutions that ensure data integrity, availability, and confidentiality in VCC environments.

3.5. Proposing Security Solutions

The research seeks to create robust security solutions that lower risks and improve the security posture of VCC systems by utilizing a thorough understanding of the threats and vulnerabilities found. The study proposes to develop a strong security framework that can address the unique challenges posed by virtual computer environments by utilizing a wide range of security measures,

including intrusion detection systems, access control mechanisms, cryptography, and secure communication protocols. The major goal is to develop security solutions that ensure data integrity, availability, and confidentiality in VCC environments.

3.6. Evaluation and Validation

Considering the proposal of security solutions, the research moves on to the critical stage of assessment and validation. The efficiency of the proposed security measures is rigorously reviewed and verified by theoretical analysis, simulations, and, where applicable, real-world experience. This method includes analyzing the impact of security solutions on system performance, usability, and scalability, as well as evaluating how well they mitigate discovered threats and vulnerabilities. The evaluation's conclusions provide invaluable information about the viability and effectiveness of the proposed security measures in real life.

Table 2: Evaluation Criteria for Security Solutions in Vehicular Cloud Computing.

Evaluation Criteria	**Description**
System Performance	Examines the impact of the suggested security fixes on the overall functionality of VCC systems.
Usability	Assesses the usability and user experience of the applied security measures.
Scalability	Evaluates the security solutions' capacity to scale successfully with expanding VCC environments.
Mitigation Effectiveness	Determines how well the planned security measures address the identified threats and weaknesses.

The VCC security solutions are evaluated according to the standards listed in Table 2. Security patch effects on system functionality are evaluated by System Performance. UX studies how users interact with the implemented changes. The ability of the solutions to grow with the expanding environment of VCC is measured by scalability. How well security mechanisms handle known threats and vulnerabilities is determined by their mitigation effectiveness.

3.7. Documentation and Reporting

This final part of the research project is meticulously documenting and assembling all of the study's findings and conclusions, including the evaluation results, threat model, vulnerabilities discovered, and security remedies proposed, into a comprehensive report. This well-written article will be an invaluable resource for researchers, practitioners, and policymakers working on vehicular cloud computing security. Furthermore, the research findings could be beneficial for scholarly publications, conference presentations, and developing best practices and industry standards.

By rigorously adhering to this methodological approach, the study seeks to provide a comprehensive and informative evaluation of the security and privacy risks associated with Vehicular Cloud Computing. The study's purpose is to make a substantial contribution to the development of effective security procedures for preserving the integrity and confidentiality of VCC systems by proposing strong security solutions and performing thorough validation.

4. RESULT AND DISCUSSION

Vehicular Cloud Computing (VCC) threat model investigation revealed important security and privacy issues, such as poor access controls, insufficient authentication, and insecure communication pathways. By applying the CIAA and STRIDE frameworks, the research methodically classified high-risk locations and identified serious risks like data breaches, GPS spoofing, and man-in-the-middle attacks. Through theoretical research and simulations, suggested security solutions—such as intrusion detection systems, encryption methods, and secure communication protocols—were assessed, proving that they could effectively mitigate threats without compromising system functionality. These solutions were improved for scalability and usability based on user feedback. Overall, this research improves the confidentiality, integrity, and availability of vehicle data in cloud environments by offering a thorough threat model and strong security techniques for VCC.

5. CONCLUSION

Finally, this work comprehensively evaluated the security and privacy concerns in Vehicular Cloud Computing (VCC) through threat model analysis and vulnerability identification. The proposed DBTEC (Double Board-based Trust estimate and Correction) method, which combines direct and indirect trust estimate, has proven to be beneficial in improving vehicle security cooperation. Through careful theoretical study and simulations, the DBTEC scheme has demonstrated considerable improvements in collaboration rates and overall system reliability. The study's complete methodology, which employs threat modeling approaches such as STRIDE and CIAA, provides a solid foundation for tackling security concerns in VCC. These discoveries help to advance secure vehicle cloud computing systems, promote safer and more efficient vehicular networks, and close important research gaps in the field. Future study could look into combining AI and machine learning to improve trust estimation accuracy, developing real-time adaptive security mechanisms, and testing the scalability of DBTEC in large-scale VCC systems. Additionally, cross-disciplinary research on policy frameworks and user privacy in VCC systems is required.

REFERENCES

1. Kashevnik, A., Ponomarev, A., Shilov, N., & Chechulin, A. (2020). In-vehicle situation monitoring for potential threats detection based on smartphone sensors. *Sensors*, *20*(18), 5049.
2. Bakhshi Valojerdi, Z., & Balador, A. (2019). An Overview on Security and Privacy Challenges and Their Solutions in Fog-Based Vehicular Application. In *2019 IEEE 30TH INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS (IEEE PIMRC WORKSHOPS), Istanbul, TURKEY, SEP 08, 2019*.
3. Shao, B., Bian, G., Wang, Y., Su, S., & Guo, C. (2018). Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment. *IEEE Access*, *6*, 43785-43797.

4. Hoque, M. A., & Hasan, R. (2019, October). Towards a threat model for vehicular fog computing. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 1051-1057). IEEE.
5. Masood, A., Lakew, D. S., & Cho, S. (2020). Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys & Tutorials*, *22*(4), 2725-2764.
6. Alamer, A., Deng, Y., Wei, G., & Lin, X. (2018). Collaborative security in vehicular cloud computing: A game theoretic view. *IEEE Network*, *32*(3), 72-77.
7. Xue, K., Hong, J., Ma, Y., Wei, D. S., Hong, P., & Yu, N. (2018). Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing. *IEEE Network*, *32*(3), 7-13.
8. Onwubiko, C. (2017, June). Security operations centre: Situation awareness, threat intelligence and cybercrime. In *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-6). IEEE.
9. Aladwan, M., Awaysheh, F., Cabaleiro, J., Pena, T., Alabool, H., & Alazab, M. (2019, August). Common security criteria for vehicular clouds and internet of vehicles evaluation and selection. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 814-820). IEEE.
10. Mishra, D., Kumar, V., Dharminder, D., & Rana, S. (2020). SFVCC: chaotic map-based security framework for vehicular cloud computing. *IET Intelligent Transport Systems*, *14*(4), 241-249.
11. Sheik, A. T., Maple, C., Watson, T., Alhagagi, H., Safa, N. S., & Woo-Lee, S. (2017, March). A threat based approach to computational offloading for collaborative cruise control. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing* (pp. 1-9).