SECURE DIGITAL FORENSICS FRAMEWORK FOR VEHICLE MAINTENANCE SERVICE RECORDS

BY

NUR SHUHADAH BINTI MOHD @ AB RAZAK

A thesis submitted in fulfilment of the requirement for the degree of Master of Computing (Computer Science and Information).

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

FEBRUARY 2024

ABSTRACT

Automotive technology is soaring and has reached an advanced phase. Despite their benefits, these advancements may expose vehicles to additional threats, particularly regarding security and data management. Currently, handling maintenance service records is a manual process, which may lead to inaccuracy, unavailability, and limited consumer access. These concerns are compounded by the lack of trustworthy platforms or legitimate sources for retrieving the history of vehicle maintenance service records. The objectives of this research are to identify a list of stakeholders to define their roles and responsibilities, to identify the security requirements that need to be implemented and to establish a secure framework and communication protocol to address these concerns. Stakeholders were identified through a snowball literature review method, and their roles were assessed to ensure comprehensive coverage of the vehicle maintenance ecosystem. The security requirements were derived using Threat and Vulnerability Risk Assessment (TVRA) and Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat modelling methodologies and then used in designing the secure frameworks and communication protocol for vehicle maintenance service records. The proposed frameworks that are designed for scheduled and repair maintenance services implement the use of consortium blockchain technology as it provides a decentralised yet controlled access to ensure that only authorised stakeholders can contribute and validate data. This approach helps to protect vehicle maintenance service records from unauthorised access and data manipulation. A secure communication protocol which mainly focuses on the grant access process for new vehicle owners was developed and then formally analysed using the Scyther Tool. This tool is chosen because of its ability to rigorously verify the security of protocols. As a result, this research listed eight stakeholders that are involved in the vehicle maintenance service records. The security requirements identified are then implemented in designing the secure frameworks and secure communication protocol to address and maintain the confidentiality, integrity and availability of vehicle maintenance service records. The integration of these solutions not only safeguards maintenance records but also supports digital forensics in providing a robust foundation for advancing the management and security of vehicle maintenance data.

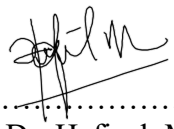
ملخص البحث

تشهد تكنولوجيا السيارات تطورًا هائلاً وبلغت مرحلة متقدمة. وعلى الرغم من فوائدها، فإن هذه التطورات قد تعرض المركبات لتهديدات إضافية، وخاصة فيما يتعلق بالأمن وإدارة البيانات. ففي الوقت الحالي، يعد التعامل مع سجلات خدمات الصيانة عملية يدوية، مما قد يؤدي إلى عدم الدقة وعدم توفر المعلومات، وصعوبة وصول المستهلكين إليها. وتتفاقم هذه المخاوف بسبب الافتقار إلى منصات موثوقة أو مصادر مشروعة لاسترجاع تاريخ سجلات خدمة صيانة المركبات. تهدف هذه الدراسة إلى تحديد قائمة بأصحاب المصلحة لتعريف أدوارهم ومسؤولياتهم، وتحديد متطلبات الأمان التي يجب تنفيذها، ووضع إطار عمل آمن وبروتوكول اتصال لمعالجة هذه المخاوف. تم تحديد أصحاب المصلحة باستخدام طريقة مراجعة الأدبيات المتسلسلة، وتم تقييم أدوارهم لضمان تغطية شاملة لنظام صيانة المركبات. تم اشتقاق متطلبات الأمان باستخدام منهجيات تقييم المخاطر والتهديدات (TVRA) ونمذجة التهديدات المعروفة بـ STRIDEوهي اختصار للتزييف والتلاعب والإنكار والإفصاح عن المعلومات ورفض الخدمة ورفع الامتيازات، ثم تم استخدامها في تصميم أطر عمل آمنة وبروتوكول اتصال لسجلات خدمات صيانة المركبات. تطبق الأطر المقترحة المصممة لخدمات الصيانة المجدولة والإصلاح استخدام تقنية اتحاد سلاسل الكتل (Consortium Blockchain) لأنها توفر وصولاً لامركزيًا ولكن خاضعًا للرقابة لضمان قدرة أصحاب المصلحة المعتمدين فقط على المساهمة والتحقق من صحة البيانات. يساعد هذا النهج في حماية سجلات خدمة صيانة المركبات من الوصول غير المصرح به والتلاعب بالبيانات. تم تطوير بروتوكول اتصال آمن يركز بشكل أساسي على عملية منح الوصول لأصحاب المركبات الجديدة ثم تم تحليله رسميًا باستخدام أداة Scyther. تم اختيار هذه الأداة نظرًا لقدرتها على التحقق

بدقة من أمان البروتوكولات. ونتيجة لذلك، قام هذا البحث بإدراج ثمانية من أصحاب المصلحة المشاركين في خدمة صيانة المركبات. تم بعد ذلك تنفيذ متطلبات الأمان التي تم تحديدها في تصميم الأطر الآمنة وبروتوكولات الاتصال الآمنة لمعالجة والحفاظ على سرية وسلامة وتوافر سجلات خدمة صيانة المركبات. لا يعمل دمج هذه الحلول على حماية سجلات الصيانة فحسب، بل يدعم أيضًا التحقيق الجنائي الرقمي في توفير أساس قوي لتعزيز إدارة وأمن بيانات صيانة المركبات.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Computing (Computer Science and Information Technology)



…….
Ts. Dr. Hafizah Mansor
Supervisor

…….
Assoc. Prof. Dr. Normaziah Abdul Aziz
Co-Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Computing (Computer Science and Information Technology)

…….
Dr. Andi Fitriah Binti Abdul Kadir
Internal Examiner

…….
Prof. Dr. Omar Zakaria
External Examiner

This thesis was submitted to the Department of Computer Science and is accepted as a fulfilment of the requirement for the degree of Master of Computing (Computer Science and Information Technology).

……
Asst. Prof. Dr. Amir ‘Aatieff bin Amir Hussin
Head, Department of Computer Science

This thesis was submitted to the Kulliyyah of Information, Communication and Technology and is accepted as a fulfilment of the requirement for the degree of Master of Computing (Computer Science and Information Technology)

……
Prof. Dr. Murni Binti Mahmud
Dean, Kulliyyah of Information, Communication and Technology

DECLARATION

I hereby declare that this thesis is the result of my investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Nur Shuhadah Binti Mohd @ Ab Razak

Signature…… Date…21st March 2025……

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

SECURE DIGITAL FORENSICS FRAMEWORK FOR VEHICLE MAINTENANCE SERVICE RECORDS

I declare that the copyright holder of this thesis/dissertation are jointly owned by the student and IIUM.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nur Shuhadah Binti Mohd @ Ab Razak

…… 21st March 2025

Signature Date

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

SECURE DIGITAL FORENSICS FRAMEWORK FOR VEHICLE MAINTENANCE SERVICE RECORDS

I declare that the copyright holder of this thesis is International Islamic University Malaysia.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may only be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purpose.

3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nur Shuhadah Binti Mohd @ Ab Razak

…… 21st March 2025 ……..

Signature Date

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

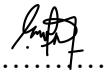
DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

SECURE DIGITAL FORENSICS FRAMEWORK FOR VEHICLE MAINTENANCE SERVICE RECORDS

I declare that the copyright holder of this thesis is Nur Shuhadah binti Mohd @ Ab Razak.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nur Shuhadah Binti Mohd @ Ab Razak



…… 21st March 2025 ……..

Signature Date

This thesis is dedicated to my parents, husband, son and family for laying the foundation of what I turned out to be in life.

ACKNOWLEDGEMENTS

All glory is due to Allah, the Almighty, whose Grace and Mercies have been with me throughout my programme. Although it has been tasking, His Mercies and Blessings on me eased the herculean task of completing this thesis.

I am most indebted to my supervisor, Asst. Prof. Ts. Dr. Hafizah Mansor, whose enduring disposition, kindness, promptitude, thoroughness and friendship have facilitated the successful completion of my work. I put on record and appreciate her detailed comments, useful suggestions and inspiring queries which have considerably improved this thesis. Her brilliant grasp of the aim and content of this work led to their insightful comments, suggestions and queries which helped me a great deal. Despite her commitments, she took time to listen and attend to me whenever requested. The moral support she extended to me is no doubt a boost that helped in building and writing the draft of this research work. I am also grateful to my co-supervisor, Assoc. Prof. Dr. Normaziah Abdul Aziz whose support and cooperation contributed to the outcome of this work.

My ultimate gratitude goes to my beloved husband, lovely son, and my parents for their prayers, understanding and endurance while away. Without that, I would not be able to endure everything up until here.

Lastly, I would like to express my gratitude to everyone who has been directly and indirectly helping and supporting me in this journey.

Once again, we glorify Allah for His endless mercy on us one of which is enabling us to successfully round off the efforts of writing this thesis. Alhamdulillah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CAN	Controller Area Network
ECU	Electronic Control Unit
OBD	On-Board Diagnostic
IoT	Internet of Things
TVRA	Threat, Vulnerability and Risk Assessment
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Over the years, technology in the automotive industry has been developing rapidly. From the advent of manual maneuverer automobiles to the ongoing development of connected cars, the automobile industry has gone through a significant evolutionary phase (Lin et al., 2016). From a simple technology application in the vehicle, we are now moving to a phase where development is focusing on the automation of the vehicles. For example, today's vehicles are equipped with more than 100 Electronic Control Units (ECUs) (Adam M., 2022).

Aside from the capacity to aid people in their daily lives, there are a few significant issues in automobile systems and services that must be tackled. There are still fraud cases related to the automotive industry such as the issues regarding vehicle data integrity and availability. Thus, the automotive sector is constantly obliged to upgrade its systems.

Vehicle digital forensics could be useful in a variety of automotive applications. For example, it can be used to store maintenance service records. Maintenance service is a component of the automobile life cycle that requires enhancements, particularly in terms of security and data management. Even though the automotive industry has evolved, most of the maintenance services are still using manual ways to keep the maintenance records which may cause inaccuracy and unavailability of data. There is also no standard method for writing service maintenance reports and confirming the integrity of the data, for example, determining whether it has been tampered with.

1.2 STATEMENT OF THE PROBLEM

Data management is an important aspect when it comes to handling a lot of data and securing important records. This includes the importance of storing vehicle maintenance service records. However, the availability of vehicle maintenance service records is a concern because the procedure is manual, which can lead to inaccuracy and unavailability of the data (Kei Leo et al., 2018). It is also difficult to ensure the integrity of the record, whether it is tampered with or not (Najdenova et al., 2019). Unless they preserve hardcopy records for the maintenance services performed on their vehicles, consumers rarely have access to these records.

The accessibility to the history of vehicle maintenance service records is important, especially for the owner, the potential buyer of the second-hand car as well as the insurance company when they need to know or check the history of the car. Moreover, there is no platform or legitimate source to retrieve vehicle maintenance service records for second-hand car buyers. This leads to the problem where vehicle information is still unreliable (Preikschat et al., 2021).

1.3 RESEARCH QUESTIONS

The problems discussed in the preceding subsection raise the following research questions (RQs), which are addressed in this study:

RQ1: Who are the responsible stakeholders for the access, upload and maintenance of the service records?

RQ2: What type of security requirements need to be included in handling the security of data?

RQ3: How to create a secure and trusted platform to store the history of maintenance service records?

1.4 RESEARCH OBJECTIVES

In answering the RQs stated in the preceding subsection, this research project seeks to achieve the following research objectives (ROs):

RO1: To identify all stakeholders and determine their roles in vehicle maintenance service records.

RO2: To study the security requirements needed in vehicle maintenance service records.

RO3: To design a secure framework and communication protocol for managing vehicle maintenance service records and supporting digital forensics.

1.5 SIGNIFICANCE OF THE STUDY

This study has a significant contribution in the automotive field specifically on the security of automotive maintenance services. Firstly, the longstanding issue of unreliable data management of vehicle maintenance service records is addressed. The issue is solved by enhancing the security of stored vehicle maintenance service records.

Secondly, this research significantly helps to improve accessibility to the history of vehicle maintenance service records. This will benefit various stakeholders such as vehicle owners, potential buyers of second-hand cars, and insurance companies.

Lastly, by establishing a legitimate source for retrieving vehicle maintenance service records for second-hand car buyers, the study contributes to rectifying the problem of unreliable vehicle information in the market (Preikschat et al., 2021). The potential buyer is assured that the car is in good condition as it is well-maintained (Ray et al., 2013). The framework's objective is to allow the car owner to keep the vehicle maintenance service record up to date, allowing them to save money on maintenance by preventing major breakdowns.

In conclusion, this research project stands as a crucial step towards a more secure, efficient, and accessible future for vehicle maintenance data management, offering valuable insights and practical solutions to the identified challenges.

1.6 CONTRIBUTIONS OF STUDY

This research project addresses the critical challenges that are related to the management of data in keeping the records of vehicle maintenance services where currently the process is handled manually. This process has led to the issues of inaccuracy, unavailability, and difficulties in ensuring data integrity. In consequence, consumers rarely have access to these records unless they are keeping the hard copies by themselves. This study undertakes a significant role in contributing to the advancement of this field by addressing the identified problems by defining the research questions and objectives. The major focus of this study is to develop a framework to store vehicle maintenance service records. This part enhances the current paper-and-pen methods for storing the data.

To achieve the major focus of this study, the first contribution of this study is to find out the stakeholders responsible for the access, upload, and maintenance of vehicle maintenance service records (RQ1). A comprehensive stakeholder identification process is

carried out and their roles are identified in detail (RO1). Secondly, the essential security requirements for handling data in vehicle maintenance service records are investigated and determined (RQ2, RO2).

Moreover, this research goes beyond mere identification and analysis by contributing to the practical aspects of data management. It designs a secure framework for vehicle maintenance service records and a secure communication protocol for digital forensics of vehicle maintenance service records (RO3). These objectives are carried out to establish a reliable and robust storage platform that addresses the concerns that have been raised (RQ3).

1.7 RESEARCH SCOPE

As emphasised in the introduction, there was no reliable platform to record vehicle maintenance service records. The concern is not only focusing on keeping the data secure but on ensuring that the data is correct from when it is being entered. There are already a few studies that have been conducted for vehicle maintenance services. However, that research is only focusing on the lifetime of the spare parts and vehicle odometers.

This study will focus on furthering the research by including the vehicle maintenance service records which will focus on car-type vehicles only. The stakeholders, their roles and related security requirements are listed at the beginning of the study. The list is crucial information and concerns in designing the frameworks. After that, a secure communication protocol is designed. Then the protocol is tested by informal and formal analysis using the Scyther tool.

However, there are a few limitations that need to be addressed. The frameworks designed are theoretically based on the identified stakeholders, their roles and security requirements. Thus, in future, the frameworks still need to be validated by the listed stakeholders to ensure the full security specification that is required is met. Other than that, this study only focuses on one secure communication protocol which is the protocol to grant access to the new owner of the vehicle. In addition, this study solely focuses on designing the framework and secure communication protocol, thus there are no applications with interfaces developed (including the blockchain interface).

In future, this research will be carried out further to test the solution using Blockchain applications to provide a more accurate and complete approach to the problem that has been discussed in Section 1.2.

1.8 SUMMARY OF RESEARCH BACKGROUND

As discussed in sections 1.2 until 1.4, a summary of research problems, research questions, and research objectives is produced as shown in Table 1.

Table 1 Summary of Research Background

Research Problems	Research Questions	Research Objectives	Expected Output
Consumers rarely have access to these records unless they keep hardcopy-based records for the maintenance services performed on their cars.	RQ1: Who are the responsible stakeholders for the access, upload and maintenance of the vehicle maintenance service records?	RO1: To identify all stakeholders and determine their roles.	List of stakeholders involved and their roles in vehicle maintenance service records management.
The history of vehicle maintenance services records is an issue since the process is manual	RQ2: What type of security requirements need to be included in handling the security of data?	RO2: To study the security requirements needed in vehicle maintenance service records.	Details of security requirements needed for vehicle maintenance service records.
There are no platforms or legitimate sources to retrieve the history of vehicle maintenance service records for 2nd hand car buyer	RQ3: How to create a secure and trusted platform to store the history of vehicle maintenance service records?	RO3: To design a secure framework and communication protocol for managing vehicle maintenance service records and supporting digital forensics.	Secure framework and communication protocol for digital forensics of vehicle maintenance service records involving all the stakeholders and considering all of the security requirements.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

The literature review is conducted by focusing on the aspects that are related to the vehicle maintenance service records. Section 2.2 highlights the challenges in the vehicle maintenance industry, while Section 2.3 focuses on the studies that highlight the stakeholders involved in the vehicle maintenance industry. Next, in Section 2.4, the literature discusses the existing framework of vehicle maintenance services, and in Section 2.5, security requirements that need to be considered are reviewed. Lastly, Section 2.6 centres on the applications of blockchain that have been suggested and implemented in the vehicle lifecycle.

2.2 CHALLENGES IN VEHICLE MAINTENANCE INDUSTRIES

The vehicle maintenance industry faces several challenges related to data security, accuracy, and availability, leading to inefficiencies, financial losses, and safety risks. Key issues include the use of counterfeit parts, fraudulent warranty claims, inaccurate predictive maintenance data, and insecure information management. These challenges highlight the need for a secure, transparent, and tamper-proof record-keeping system to ensure trust, accountability, and reliability in vehicle maintenance service records.

A problem in vehicle maintenance service is highlighted when counterfeit spare parts are usually found in the workshop (Meyliana et al., 2021). This fact leads to the

assumption that counterfeit parts might be used when customers come to receive maintenance service from those workshops. It is a concern that needs to be addressed. It does not matter whether the counterfeit parts are being used in the knowledge of the customers or not since it can lead to many problems in the future especially when the vehicle is being sold to another person. Thus, their research attempts to use blockchain technology to track automobiles for spare parts being used in vehicle maintenance service records. Another challenge in vehicle maintenance services is the possibility of fraud in managing the warranty claims of remanufactured or repaired components (Pandit & Gupta, 2021). This type of fraudulent claim can occur when vehicle owners try to replace the parts that are already out of warranty by falsely claiming they are still covered under warranty. This issue can lead to a bigger problem where it leads to financial losses for manufacturers and inaccuracies in maintenance records. Then, the product reliability assessments and warranty cost predictions will be inaccurate. Manufacturers rely on accurate maintenance data to track if there are any failures in the components as well as to improve product designs. A study by Pandit and Gupta (2021) highlighted that integrating embedded sensors into vehicle components can improve fraud detection since it helps to reduce false claims by 25.8%.

This challenge underscores the need for secure and tamper-proof vehicle maintenance records because manipulated service histories can mislead potential buyers, impact insurance assessments and create safety risks due to unverified repairs. Emerging technologies, such as blockchain, provide a promising solution by ensuring data authenticity, preventing unauthorised modifications, and enhancing traceability in vehicle servicing processes. By leveraging blockchain's immutability and distributed ledger properties, fraudulent alterations to maintenance records can be mitigated, ensuring transparency and reliability in the vehicle maintenance industry.

Another critical challenge for vehicle maintenance services is to predict maintenance costs as explored by Zhonghui et al. (2023). They used the Weibull model to

analyse data from multiple vehicle sales batches to create a reliable model for cost prediction. While their research successfully developed a reliable model, the study emphasised that the integrity of maintenance records data is still a concern that needs to be addressed as a vital factor influencing the reliability of their model. The data fed into the predictive models requires a high level of integrity to avoid any flawed outcomes.

This reinforces the need for a system that guarantees the accuracy and security of maintenance service records which is an objective that this study seeks to achieve. By ensuring that maintenance records are securely stored and resistant to tampering or unauthorised modifications, the proposed framework will address this data integrity challenge to enable better integration with predictive maintenance models like those proposed by Zhonghui et al.

In addressing the broader issue of vehicle sales and maintenance management, Rahul et al. (2022) proposed a car and motor sales management information system that collects, stores, transfers, and processes automobile sales information. They implemented an encryption algorithm using the Model-View-Controller (MVC) architecture to secure the data. However, MVC has its limitations where its scalability and efficiency have reduced and are not reliable anymore to be applied in modern applications. The newer Model-View-View-Controller (MVVC) architecture has been introduced to address some of these drawbacks by providing a more robust structure for managing complex systems. While their work primarily focuses on sales management, their emphasis on encryption and data security highlights the broader relevance of secure architecture in related domains, such as vehicle maintenance service records. This research builds upon such concepts by designing a secure communication protocol for vehicle maintenance service records to ensure that data remains protected during transmission and storage.

Other than that, one of the critical challenges in vehicle maintenance industries is the use of counterfeit and fraudulent auto parts that can compromise the reliability and

safety of vehicles. Many accidents are caused by substandard components but existing supply chain systems still lack in term of transparency and reliable mechanisms for verifying the authenticity of vehicle parts. Traditional centralised databases are vulnerable to data tampering, making it difficult to ensure accurate records of vehicle maintenance and repairs (Chen et al., 2021). Additionally, despite regulatory efforts to limit counterfeit parts and illegal modifications, fraudulent practices still occur due to weak enforcement and ineffective tracking systems. To address these issues, Chen et al. (2021) proposed a blockchain-based traceability system that enhances security, transparency, and authenticity in vehicle maintenance records and parts management. The system leverages smart contracts to automate verification and transactions to reduce human error and fraud risks by integrating the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure that maintenance records and part histories remain tamper-proof. Furthermore, the decentralised nature of blockchain enhances end-to-end traceability that allows stakeholders including manufacturers, dealers, and service providers to verify the legitimacy of vehicle components at every stage. This study highlights the necessity of adopting blockchain technology in the automotive industry to safeguard data integrity, prevent fraudulent claims, and enhance trust within the ecosystem (Chen et al., 2021).

In conclusion, there are severe challenges that are currently happening in the vehicle maintenance industry. The challenge includes the use of counterfeit parts, fraudulent warranty claims, inaccurate predictive maintenance data, and insecure information management. Thus, the vehicle maintenance service industry critically needs a secure and tamper-proof record-keeping system. Existing solutions such as blockchain-based traceability systems, predictive models, and encrypted sales management platforms help to improve security and data integrity in vehicle maintenance processes. However, many of these approaches still do not have secure mechanisms to ensure data authenticity, availability, and secure access control. Thus, this research builds upon these studies by proposing a secure framework and communication protocol designed specifically for vehicle maintenance service records. The summary of the literature review for vehicle maintenance service is summarised in Table 2.

Table 2 Summary of Literature Review for Vehicle Maintenance Service

Title	Author	Publication Year	Problems / Objectives	Approach
Maintenance cost prediction for the vehicle based on maintenance data	Zhonghui et al.	2023	To predict the cost of vehicle maintenance service based on the maintenance data	Design a model to predict the cost of maintenance service. However, the maintenance record data is not reliable
Car & Motor Vehicles Sales and Maintenance	Rahul et al.	2022	To propose a car and motor sales management information system.	Design an encryption algorithm to secure the data by applying a Model-View-Controller (MVC) architecture in developing their application.
Blockchain Technology for Vehicle Maintenance Registration	Meyliana et al.	2021	To track automobiles for spare parts being used in vehicle maintenance services.	Use blockchain technology to track automobiles for spare parts being used in vehicle maintenance service.
Tackling Substitution	Pandit et al.	2021	To highlight the issue of	Improve the existing method of

Fraud in Remanufactured Product Warranty Service			remanufactured product warranty frauds arising from the customer specifically those related to the consumer electronics remanufacturing sector.	fraud prevention and detection by considering the implementation of sensors in the remanufactured products.
A Secure and Traceable Vehicles and Parts System Based on Blockchain and Smart Contract	Chen et al.	2021	To find the solution of counterfeit and fraudulent auto parts and data tampering in centralised systems for vehicle parts and tracking.	Implement the symmetrical Blockchain's digital ledger and smart contract technology to build a decentralised supply chain system

2.3 STAKEHOLDERS IN THE VEHICLE MAINTENANCE INDUSTRY

Several works discuss the vehicle lifecycle process, including vehicle maintenance services. Their discussion mentioned the stakeholders involved in the process. The stakeholders involved in vehicle maintenance services are consumers, automakers, repair shops, and insurance companies (Kei Leo et al., 2018).

In discussing Malaysian stakeholders' views and future research needs regarding the factors of end-of-life vehicle recovery, the research highlighted five main stakeholders related to the industries. The stakeholders are automotive spare part dealers, service centres, scrap metal handlers, remanufacturers, and policymakers (Mohamad Ali et al., 2018).

Lastly, the stakeholders' perceptions of the automotive aftermarket forecast in a changing world are discussed. The study considered six groups of stakeholders involved in maintenance services, where group one the stakeholders include repair shops, bodywork shops, and painting, while the second group includes electronic and maintenance shops (Laborda et al., 2020). The study also considered insurance companies, spare parts and post-sales consultants as stakeholders.

In the context of ensuring the accuracy, integrity, and availability of vehicle maintenance records, stakeholders play a crucial role. Each stakeholder contributes to the maintenance ecosystem by generating, verifying, or managing vehicle data. Therefore, stakeholders act as key parameters that influence the security and reliability of the records.

2.4 EXISTING FRAMEWORKS IN VEHICLE MAINTENANCE INDUSTRIES

Najdenova (2019) introduced a decentralised solution using the ByzCoin blockchain protocol and the Calypso framework to eliminate fraud in the automotive industry. This approach aims to establish trust among stakeholders that include vehicle owners, potential buyers, car manufacturers, garages, insurance companies, and car dealers. Confidential data is stored on the blockchain to ensure data immutability and security. However, the study only offers a little insight into the management of maintenance records that need to be

updated frequently, especially on the data validation systems. The validation of data is essential for guaranteeing the integrity of maintenance records.

Brousmiche et al. (2018) proposed a Blockchain-backed Vehicles Data and Processes Ledger framework to manage vehicle life cycles and data histories as shown in Figure 1. Their framework emphasises transparency and collaboration among stakeholders for better traceability throughout the vehicle lifecycle. While the framework effectively demonstrates the benefits of using blockchain for lifecycle data, it does not directly address challenges in managing and securing vehicle maintenance service records. The proposed system primarily focuses on static historical data, leaving a gap in ensuring the reliability and security of ongoing maintenance updates.

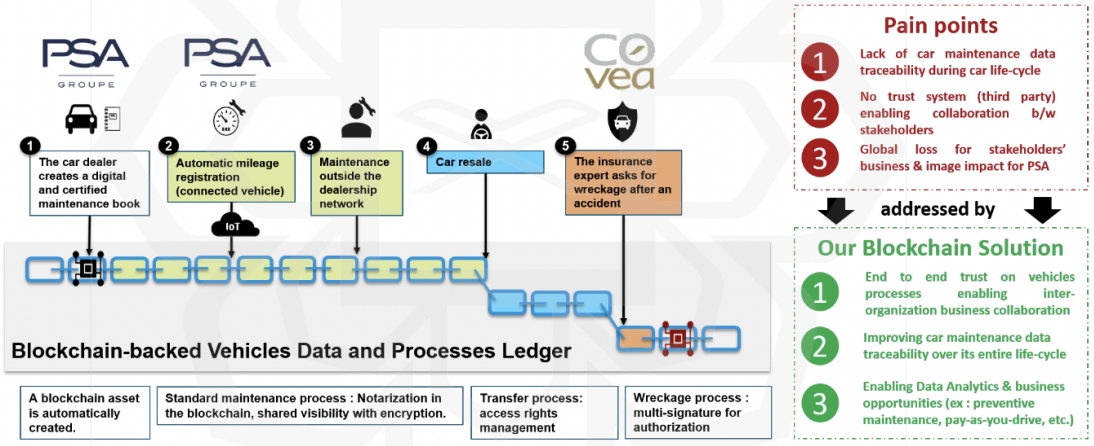


Figure 1 Digitalising Vehicle Life-cycle over a Consortium Blockchain: Pain Points and Benefits of our Framework (Brousmiche et al., 2018)

Lin et al. (2020) presented a blockchain-based platform for integrating Usage-Based Insurance (UBI) with maintenance services. Their system records driving data on the blockchain to improve premium calculations based on factors such as driving distance, time, and area. As the maintenance service records and insurance services are mainly related, thus they proposed a flowchart for the insurers to analyse the vehicle's risk based

on vehicle maintenance service records as shown in Figure 2. However, while the platform integrates blockchain for data storage, it lacks a detailed framework for managing secure communication and data validation between stakeholders. The focus remains on insurance-related metrics rather than the broader context of maintenance records.

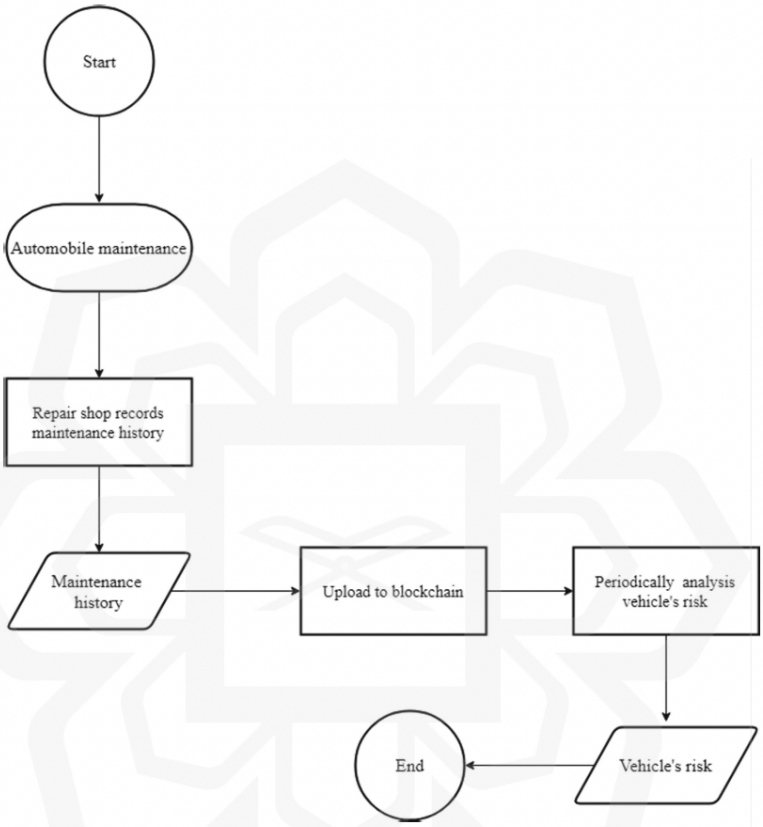


Figure 2 Flowchart of Insured Automobile's Risk Analysis (Lin, W-Y et al., 2020)

In summary, although current blockchain applications have made great progress in handling issues in the automotive sector, they still have severe drawbacks that reduce their usefulness for maintaining maintenance service records. For example, frameworks proposed by Najdenova (2019) face limited scalability and weak data validation during entry. Solutions such as Brousmiche et al. (2018) focus primarily on static data only where each data is updated manually by the service provider thus the integrity of the data is

questionable. Additionally, platforms like Lin et al. (2020) reveal communication security gaps, leaving interactions between stakeholders vulnerable. Table 3 below shows the comparison of existing frameworks in vehicle maintenance industries.

Table 3 Comparison of Existing Frameworks in Vehicle Maintenance Industries

Title	Author & Publication Year	Description	Advantages	Disadvantages
An On-Board Equipment and Blockchain-Based Automobile Insurance and Maintenance Platform	Lin et al. (2020)	A blockchain-based platform integrating Usage-Based Insurance (UBI) and maintenance services.	Utilises blockchain for insurance premium calculations. Links maintenance records with insurance services.	Focuses narrowly on insurance metrics. Lacks secure communication and robust data validation mechanisms.
Blockchain-Based Approach for Preserving Car Maintenance History	Najdenova (2019)	Decentralised solution using ByzCoin blockchain protocol and Calypso framework to eliminate fraud.	Ensures data immutability and security. Builds trust among stakeholders.	Limited scalability. Insufficient focus on frequently updated maintenance

				records.
Digitizing, Securing and Sharing Vehicles Life Cycle Over a Consortium Blockchain: Lessons Learned	Brousmiche et al.	Blockchain-backed Vehicles Data and Processes Ledger framework for managing vehicle life cycles.	Enhances transparency and collaboration. Improves traceability across vehicle lifecycles.	Focuses on static data; lacks mechanisms for managing dynamic maintenance updates. Manual data entry affects data reliability.

2.5 SECURITY REQUIREMENTS

There are a few security requirements that need to be considered in the process of developing the framework for vehicle maintenance service records.

To achieve a secure, reliable, and accessible vehicle maintenance system, the following security requirements serve as critical parameters that guide system design. These parameters define the necessary protections to ensure that records remain trustworthy and available to authorised stakeholders.

2.5.1 Confidentiality

In designing a framework for vehicle maintenance service records, ensuring confidentiality is crucial to protect sensitive information from unauthorised access or disclosure (Kei Leo et al., 2018; Kieseberg et al., 2016). Confidentiality can be achieved by implementing strict access controls to the users to restrict access to the system only for authorised personnel. Other than that, the communication needs to be encrypted during the transmission and storage to prevent unauthorised parties from deciphering any sensitive information.

2.5.2 Integrity

Data integrity is the accuracy, consistency, and security of the data throughout its lifecycle. This is to ensure the trustworthiness of the underlying data (Kei Leo et al., 2018; Kieseberg et al., 2016; Bharati et al., 2020). In the car maintenance service, data integrity refers to the originality and authenticity of the data from the time it is stored to the time it is updated until the data is no longer usable (Butera et al., 2023; Buquerin et al., 2021). The structure should ensure the data is immutable. Immutable means that once the data has been entered, no stakeholder should be able to change, edit, or delete it. If there are any revisions, the record is recorded in the new block in the blockchain.

2.5.3 Data Availability

Next, the security requirement needed in keeping the data for vehicle maintenance service records is the availability of data. The users should have access towards the data (Butera et

al., 2023; Bharati et al., 2020). In terms of data availability, vehicle maintenance service records should be accessible in reading mode when required.

2.5.4 Non-repudiation

An important security requirement in a logging system includes non-repudiation (Butera et al., 2023). Non-repudiation is to ensure all parties involved cannot deny their participation in the communication process. For example, an authorised user needs to have a unique signature or identifier upon enrolment. It is important to track the updated information and keep the information safe, considering the details of those who input the information are traceable. As vehicle maintenance services records include multiple stakeholders, strict standard operating procedures are needed in granting and revoking access to the stakeholders.

2.5.5 User Authentication

User authentication is the process where the identity of an individual who attempted to access the system is verified. It is to ensure that the person claiming to be a specific user is indeed that user (Butera et al., 2023). It is important to prevent unauthorised access and protect sensitive information.

2.5.6 Data Authentication

The authenticity of the records that have been stored is defined as data authentication. Data authentication is the process of verifying the integrity and origin of data to ensure that it has not been tampered with or altered. The vehicle maintenance service records should be original, written by the correct person, and contain accurate data (Buquerin et al., 2021).

2.6 BLOCKCHAIN IN-VEHICLE APPLICATIONS

Recently, both industry and academia have conducted extensive blockchain research related to its application in the automotive industry (Abbade et al., 2020; Elagin et al., 2020). Blockchain is a distributed ledger that consists of blocks of data that are linked together through a chain (Li et al., 2013). Once a new record is made, a new block is created where it is linked using a hash to the previous data in the previous block. The data recorded in the blockchain is safe without any tampering as blockchain provides immutability, transparency, and data encryption (Xu et al., 2021; Dorri et al., 2017). There are four types of blockchain which are public, private, hybrid and consortium blockchain (Kathleen et al., 2021). Due to the character of decentralisation, openness, and tamper resistance of blockchain, its technology has been viewed as a possible solution for the management of distributed Internet of Things (IoT) devices (Yeh et al., 2023).

Blockchain technology involves a public distributed ledger, data encryption, proof of work, and data mining. A distributed ledger is a data structure that contains an ordered list of transactions. It is a database that is shared, replicated, and synchronised among members of a decentralised network with no participation from a third party. Each record added to the ledger will have a timestamp and a unique cryptographic signature. Because

the record is shared with all network participants, any attempt to change or tamper with it is impossible.

Additionally, blockchain's robust cryptographic protocols enable secure access control to ensure that only authorised stakeholders such as manufacturers, workshops, insurers, and vehicle owners can view or update records. This feature fosters seamless collaboration without compromising security or privacy. For example, repair shops can update maintenance histories, insurers can validate records for claims, and vehicle owners can access verified service data all within a trusted and unified environment.

While existing systems often rely on centralised control, blockchain can help the system to apply decentralised control and its secure nature. Its application will be better suited for the complexities of managing vehicle maintenance service records. Its ability to address challenges like data integrity, access control, and stakeholder collaboration highlights its relevance and value in this context.

Blockchain also addresses the challenges of integrating data from multiple sources such as diagnostic tools, repair workshops and manufacturers. Its transparent ecosystem validates and traces every update, improving data reliability and simplifying dispute resolution in scenarios like warranty or insurance claims.

The application of blockchain framework for the automotive industry in a smart city is discussed (Sharma et al., 2019). The research highlighted that one of the most serious problems in the automotive supply chain is counterfeiting, which is now estimated to be worth several billion dollars in spare parts. As a solution, they suggest a blockchain framework that enables the compilation of secure digital product memory records throughout the supply chain lifespan. It begins before assembling the raw materials into parts and continues through production, maintenance, and recycling.

Permissioned blockchain focuses on managing the collected vehicle-related data to provide comprehensive forensic services in case of an accident or any legal inquiries are discussed (Cebe et al., 2018). The proposed blockchain consists of five different types of nodes which are clients, law enforcement, maintenance service providers, insurance companies and car manufacturers.

A survey on blockchain for the automotive industry is conducted (Fraga-Lamas et al., 2019). It covers blockchain design, deployment, and optimization. The survey identifies key benefits blockchain can provide, which include tamper-proof data, no single point of failure, privacy, stakeholder identity management, smart contract enforcement, and autonomy. They discussed how blockchain is a real aid to the automotive industry, as well as examples of how to utilise it, where to apply it, and what the benefits are.

A consortium blockchain is proposed to be applied as a security measure in managing vehicles' life cycle records (Brousmiche et al., 2018). Instead of using a private blockchain, which only involves one organisation and has a centralised architecture, consortium blockchain allows numerous organisations to participate. The concept encourages data sharing and collaboration among automobile sector players.

In conclusion, blockchain's decentralised model is well-suited to the complexities of vehicle maintenance service records. The summary of the literature review for blockchain in vehicles is listed in Table 4. By addressing challenges in data integrity, secure access, and stakeholder collaboration, blockchain not only ensures the long-term reliability of records but also fosters a more transparent and efficient vehicle maintenance ecosystem.

Table 4 Summary of Literature Review for Blockchain in Vehicles

Title	Author	Publication Year	Problems / Objectives	Approach
Technological Aspects of Blockchain Application for Vehicle-to-network	Elagin et al.	2020	There is no system for integrating data from all parties including other vehicles, road conditions, manufacturers, and maintenance centres.	Permissioned blockchain technology implements shared and fragmented ledgers to securely and efficiently exchange information between the collaborating parties.
Blockchain-Based Distributed Framework for the Automotive Industry in a Smart City	Sharma et al.	2019	There are many security vulnerabilities and incapable of providing secure data sharing.	A blockchain framework that enables the compilation of secure digital product memory records throughout the supply chain lifespan
A Review on Blockchain Technologies for an Advanced and	Fraga-Lamas et al.	2019	Conducted a survey on blockchain for the automotive industry that covers	Blockchain application is a real aid to the automotive industry.

Cyber-Resilient Automotive Industry			blockchain design, deployment, and optimisation	Vehicle maintenance is a service that needs the blockchain as an enhancement to be implemented.
Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles	Cebe et al.	2018	Provide comprehensive forensic services in case of accident or any legal inquiries	Permissioned blockchain to manage the collected vehicle-related data.
Digitizing, Securing and Sharing Vehicles Life Cycle Over a Consortium Blockchain: Lessons Learned	Brousmiche et al.	2018	Vehicle odometer fraud is becoming a growing problem internationally	Consortium blockchain as a security measure in vehicles' life cycle.

CHAPTER THREE

METHODOLOGY AND RESEARCH DESIGN

3.1 INTRODUCTION

This chapter is going to explain in detail the process that needs to be carried out in this research to solve the problems and achieve the objectives and goals which includes a comprehensive overview of the research activity flowchart, research methodology, and experimental procedure.

This chapter aims to offer a holistic understanding of the systematic approach undertaken to address the research objectives, contributing to the advancement of knowledge in this field of study.

3.2 RESEARCH ACTIVITIES FLOWCHART

The initial phase of this research flowchart activity begins with the conceptual groundwork that needs to be done at every start of research and development which focuses on identifying the problems and challenges in the industries This process helps to identify the best solutions and approaches that can be considered and applied.

Next is the process of identifying stakeholders and defining their respective roles within the research framework. This step is crucial since the stakeholders have important roles in ensuring the safety of vehicle maintenance service records management.

The subsequent stage is to gather the security requirements that need to be taken into consideration in designing the framework.

With requirements in hand, the flowchart advances to the design phase where the process of designing the framework and protocol takes place. The design process is carried out by integrating the identified requirements.

In parallel with the design process of framework and protocol, analysis is carried out by conducting informal and formal analysis to check whether the design meets the requirements that have been listed beforehand. If the criteria are met, the research progresses to the finalisation phase which is preparing the documentation and publication of results. This step will help to contribute to the broader academic and professional community by sharing valuable insights.

However, if the evaluation indicates that certain requirements are not satisfied, the flowchart incorporates a feedback loop which will direct the process back to the framework design stage. This iterative approach allows the framework and protocol to be refined and enhanced continuously until it aligns with the identified requirements.

To ensure that each phase of the research aligns with the objectives and addresses the identified challenges, a checklist-based validation approach is adopted. Each phase such as stakeholder identification, security requirements gathering, and framework design, is

validated against specific criteria to confirm its completeness and relevance. The research activities flowchart that is conducted in this research is represented in Figure 3.

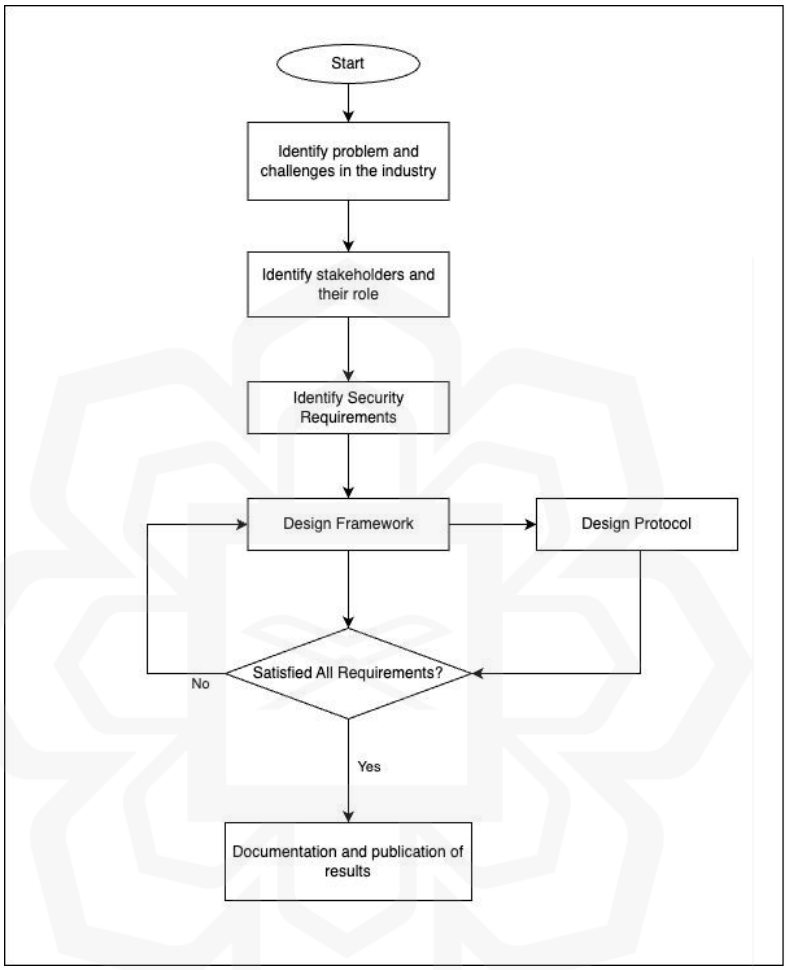


Figure 3 Research Activity Flowchart

3.3 EXPERIMENTAL PROCEDURE

3.3.1 List Stakeholders and Define Roles

After assessing the problems and challenges in vehicle maintenance service records, this study began by identifying the list of stakeholders and defining their roles in vehicle maintenance service records. This process is carried out by doing reviews of the existing papers and research focusing on the vehicle maintenance industries. From the list of stakeholders that are highlighted in existing studies as described in Section 2.3, a comparison is made to identify the stakeholders related to vehicle maintenance service records management.

In total, eleven stakeholders have been highlighted in the existing papers and summarised as shown in Figure 4. The stakeholders are insurance companies (Kei Leo et al., 2018, Mohamad Ali et al., 2018, Laborda et al., 2020), electronic and maintenance services, repair shops (Kei Leo et al., 2018 and Laborda et al., 2020) and dealerships (Mohamad Ali et al., 2018 and Laborda et al., 2020). Other than that, the papers also listed customers and manufacturers (Kei Leo et al., 2018) as well as remanufacturers, scrap metal handlers and legislators (Mohamad Ali et al., 2018). Lastly, spare parts and post-sale consultants are also considered vehicle maintenance stakeholders (Laborda et al., 2020).

However, this study narrows its focus to stakeholders with direct involvement in the life cycle of vehicle maintenance service records to ensure relevance to the research scope. Seven key stakeholders are included which are vehicle manufacturers, dealers that include post-sale consultants, vehicle owners, repair shops that include spare parts shops, technology teams, insurance companies, and legislators. These stakeholders were selected

based on their roles in generating, maintaining, or accessing maintenance records, as well as their impact on the security and operational aspects of the system.

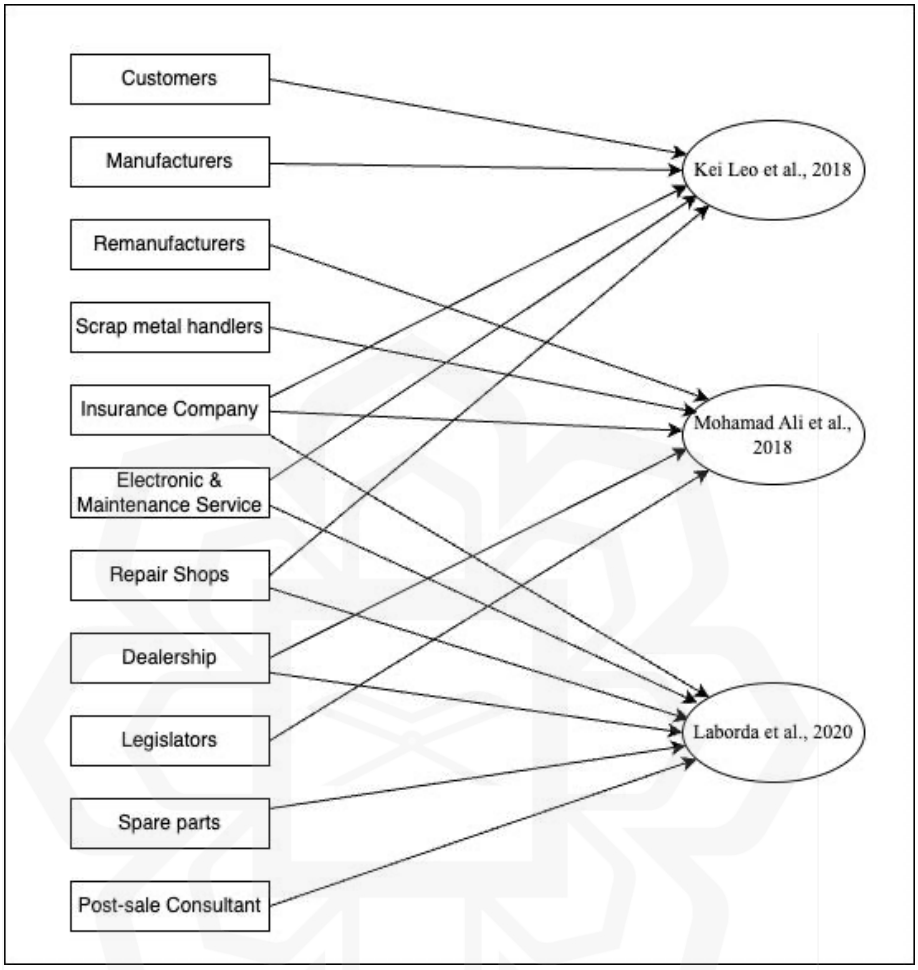


Figure 4 List of Stakeholders Highlighted in the Existing Research

To streamline the stakeholder list, some groups were grouped according to their operational overlap. Post-sale consultants were grouped under dealerships since they operate within the dealership framework and play a key role in maintaining customer relationships and assisting with maintenance records. Similarly, spare parts shops were integrated under repair shops as they provide the essential parts needed for vehicle repairs and are intimately related to workshop operations.

Legislators were eventually acknowledged as crucial stakeholders after first being excluded because of their indirect involvement in day-to-day vehicle maintenance service records activities. Their role in establishing data protection laws, standardization policies, and compliance frameworks ensures that the proposed system aligns with industry regulations and legal standards.

Certain stakeholders were excluded to refine the scope of this study. Remanufacturers were excluded as their role focuses primarily on refurbishing and reconditioning vehicle components which is more aligned with part lifecycle management rather than vehicle maintenance service records. Other than that, scrap metal handlers were excluded because they are indirectly involved in the vehicle lifecycle. They primarily focus on part recycling and disposal during the end-of-life phase of vehicles only. Their limited relevance to the generation, security, or management of maintenance records led to their exclusion.

Identifying relevant stakeholders plays a crucial role in ensuring the accuracy of vehicle maintenance service records. A clear role and responsibilities help to guarantee that each record update comes from an authorised and credible source. For instance, manufacturers are responsible for providing initial vehicle data such as its specifications and part serial numbers. Other than that, repair shops are required to update the records after performing maintenance or part replacements to ensure that these records reflect actual service activities. Similarly, insurance companies validate claims and verify that services are recorded accurately. This process ensures that the records are updated only by verified entities, reducing the risk of inaccurate or fraudulent entries.

3.3.2 Identify Security Requirements

The development of a secure framework for vehicle maintenance service records requires meticulous consideration of security requirements which has been highlighted and concerned in a few related literature. To ensure the trustworthiness of vehicle maintenance records, the system must meet several security requirements. These requirements serve as parameters to maintain the accuracy, integrity, and availability of records, guiding the development of the framework and protocol.

The first security requirement is non-repudiation which emphasises the irrefutability of actions (Butera et al., 2023). In addition, the integrity of data is an important aspect of security requirements for data logging systems to ensure the reliability and trustworthiness of the data (Butera et al., 2023; Kei Leo et al., 2018, Kieseberg et al., 2016; Bharati et al., 2020, Buquerin et al., 2021). Additionally, it is crucial to guarantee the availability of data to be accessed by the user (Butera et al., 2023 Bharati et al., 2020). User authentication is a vital component to restrict access and maintain system security (Butera et al., 2023).

Finally, data authentication plays a crucial role in ensuring the validity and authenticity of the recorded information (Buquerin et al., 2021). By incorporating these security requirements, the proposed framework aims to establish a secure and dependable foundation for the management of vehicle maintenance services records.

3.3.3 Threat Modelling

Threat modelling steps are conducted in this research as an informal analysis to identify and understand the threat and its impacts on vehicle maintenance service records management. This process is a source of help in finding the best security measure that needs to be applied in designing a framework and creating a system protocol. Threats are potentially malicious occurrences that threaten the confidentiality, integrity, and/or availability of information systems. Thus, threat modelling will assist in identifying, understanding, and giving insights into the possible threats that might affect an organisation or system.

In this study, a combined approach using Threat, Vulnerability and Risk Assessment (TVRA) and Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) were chosen. TVRA offers a detailed, risk-based assessment of potential vulnerabilities, while STRIDE complements this by categorising threats into specific types. This combination offers a comprehensive perspective on the threat landscape, ensuring that potential risks are fully addressed. STRIDE serves as a checklist to systematically identify threats like tampering with maintenance records, spoofing stakeholders such as vehicle owners or repair shops, and disclosing sensitive vehicle history data. Together, these methodologies enhance the overall understanding of threats relevant to the system.

The threat modelling process began with the TVRA methodology, which included three key steps. The first step is identifying the critical aspects within the system such as maintenance records and user authentication data. The process focused on critical aspects within the vehicle maintenance service records system, such as the confidentiality of maintenance data, the integrity of service logs, and the availability of historical records for stakeholders like repair shops, vehicle owners, and insurers. Key assets included

authentication credentials, maintenance schedules, vehicle condition records, and warranty data.

Next, a vulnerability analysis was conducted to examine if any weaknesses might lead to possible threats. For example, the analysis looked at vulnerabilities in areas like authentication, data integrity, and communication protocols that attackers might exploit. One major vulnerability is the presence of weak authentication mechanisms, which could enable unauthorised entities to access sensitive vehicle records. Another significant concern involves insufficient safeguards against tampering with maintenance logs, where malicious actors might modify repair histories or falsify part replacement details. Additionally, vulnerabilities in communication protocols can increase the risk of man-in-the-middle attacks during the transmission of maintenance data between stakeholders. These weaknesses highlight the need for robust security measures to protect the integrity and confidentiality of vehicle maintenance service records.

A risk assessment was carried out to determine the potential impact of various threats. This assessment led to a prioritized list of threats categorized as high, medium, or low impact, guiding mitigation efforts. The impact level of a threat is determined by the severity of its consequences on vehicle maintenance service records. High-impact threats result in significant financial loss, legal repercussions, regulatory penalties, reputational damage, or safety hazards. These threats demand immediate attention and mitigation efforts. Medium-impact threats may disrupt operations by causing service delays, or result in moderate financial and reputational damage. While not as critical as high-impact threats, they require proper management to prevent escalation. Low-impact threats cause minor inconveniences, such as usability issues or slight inefficiencies, and can typically be addressed through routine security improvements.

The likelihood of a threat occurring in vehicle maintenance service records is assessed based on its probability and frequency of occurrence. In this research, likelihood

is categorized into three levels which are low, medium, and high**.** A low likelihood indicates that the threat is rarely observed in existing research or industry cases, requiring specific conditions or advanced attack methods. A medium likelihood suggests that the threat has been identified in multiple studies or industry reports, but its occurrence depends on specific factors such as weak security controls or insider threats. Meanwhile, a high likelihood signifies that the threat has been frequently reported in real-world cases, making it a critical concern due to its ease of exploitation or widespread impact across the vehicle maintenance ecosystem.

It is important to note that these likelihood ratings are based on assumptions derived from existing literature, industry reports, and documented security incidents. While they provide an initial understanding of potential risks, further validation is necessary to enhance accuracy. A more comprehensive study, involving direct engagement with relevant stakeholders including manufacturers, repair shops, insurers, and policymakers would offer deeper insights into the actual risk landscape. Future research should incorporate empirical data, industry surveys, and real-world case studies to refine these likelihood assessments, ensuring they accurately reflect the security challenges in vehicle maintenance service records.

The identified threats, vulnerabilities, and risk levels from the TVRA process are presented in Table 5. The table includes columns for the threat description, associated vulnerability, risk assessment of the possible impacts, and a suggested mitigation strategy. For example, a possible threat such as unauthorised login is associated with a vulnerability in weak authentication which leads to high impact. A suggested mitigation for this particular threat could be the implementation of Two-Factor Authentication (2FA).

By integrating findings from both TVRA and STRIDE, the threat modelling approach in this study provided a holistic view of the potential risks and vulnerabilities. TVRA contributed an in-depth analysis of the risk level and impact of threats, while

STRIDE's systematic categorisation ensured comprehensive coverage. This combined approach allowed for a well-rounded understanding of the threat landscape, enabling a stronger, more informed security strategy for the system under study.

Table 5: Threat Modelling using TVRA and STRIDE methods

Threat ID	Threat Description	Vulnerability	Risk Level (Likelihood /Impact)	Mitigation	STRIDE Category
1	Unauthorised login	Weak authentication	Medium/ High	Two-factor authentication (2FA) with secure communication protocol	Spoofing
2	Unauthorised data modification	Weak data integrity	High/High	Encryption, data validation	Tampering
3	Records alteration	Store records in editable format	High/High	Blockchain implementation	Tampering
4	Falsified records update	Lack of verification of actual maintenance tasks	Medium/ High	Extract data from ECU before and after service to validate data	Tampering

5	Unauthorised and unverified new data	Lack of verification of data authenticity and its sources	High/High	Each record can be updated only by an authorised user with a credential	Repudiation
6	Records deletion	Systems allow data deletion	High/High	Blockchain implementation	Repudiation
7	Data leak due to interception	Unencrypted data transmission	Medium/ High	Encryption during transmission	Information Disclosure
8	Malicious actors inject false or manipulated data into a system	Insufficient integrity and authenticity checks on incoming data expose	Medium/ High	Blockchain implementation and data authentication	Denial of Service
9	Impersonation enables unauthorised access to sensitive data	Lack of robust authentication mechanisms	High/High	Implementation of secure communication protocol	Elevation of Privilege

3.3.4 Framework Design

After the literature review and information gathering have been conducted, the findings are used in designing a secure framework together with the implementation of security measures. The process includes the research on listing the stakeholders involved in the vehicle maintenance service records, their roles and security requirements that need to be included in the framework. Hence, the list and details of stakeholders are considered and applied accordingly in the design of a secure framework that provides the necessary security goals for the maintenance services records. The process of designing and validating the framework and protocol in this research is summarised in Figure 5.

In designing the framework, blockchain technology is applied. From the various types of blockchain, consortium type of blockchain is chosen based on its characteristics. A consortium blockchain is a type of blockchain network where multiple organisations or entities collaborate to maintain and operate the network. Unlike public blockchains where access is open to anyone, and private blockchains where a single entity controls the network, a consortium blockchain involves a group of organisations that work together in a decentralised manner which is very applicable to the research since vehicle maintenance service records management involves multiple groups of organisations.

By applying a consortium blockchain that involves multiple participants several organisations listed as the stakeholders of vehicle maintenance service records can join the network and have the authority to validate transactions and maintain the blockchain. This will allow the control to be decentralised because the control of the blockchain is distributed among the participating organisations.

Lastly, consortium blockchains are usually permissioned which means the participants are known entities and have permission to access and validate transactions

only. This allows the governance of the blockchain to be shared among the consortium members, and decisions related to the network's rules and protocols are typically made collectively to foster a more decentralised structure compared to private blockchains.

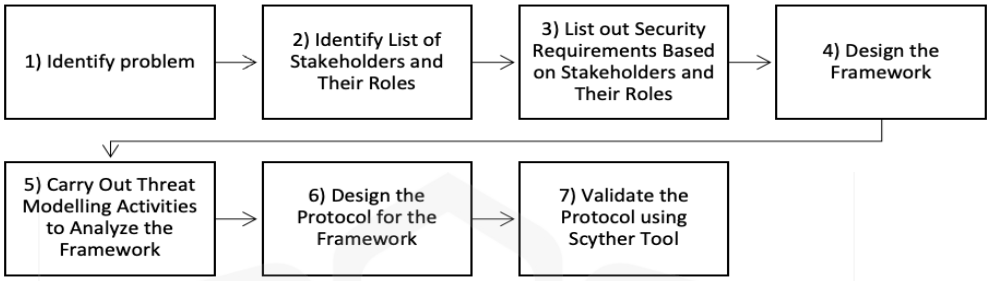


Figure 5 Process Involved in Designing the Framework and Protocol

3.3.5 Protocol Design

After designing the framework and conducting a comprehensive analysis of threats to the system, the next step is to develop a secure communication protocol. There are a few series of protocols that need to be designed to cover all the communication that might happen in the framework. The aim of this is to ensure that the communication and data involved are secure from any threat.

A sequence diagram is created to illustrate the communication included in the process of developing the secure communication protocol. Sequence diagrams are used to create a protocol for specific interactions. The focus of the sequence diagram in this study primarily revolves around the initial steps required to grant access to the new owner as shown in Figure 6.

Once the potential buyer's decision to acquire the vehicle is confirmed, the dealer is responsible for facilitating access for the new owner. The process begins with dealers logging into the system and undergoing an authentication procedure to validate their status as authorised dealers. Subsequently, once the system receives the activity initiated by the dealer, the update on the newly generated activity is sent to the blockchain system. Simultaneously, the blockchain system acknowledges the communication, confirming its approval and recording the transaction. This acknowledgement is reciprocally transmitted to the system, serving the same purpose.

Following this initial stage, the dealer is prompted to add the vehicle's ID, which is assigned to the new owner. Upon receiving and validating the ID, the system will request the selling details from the dealer which is considered a necessary step to verify the legal sale of the vehicle to the new owner. In response to the system's request, the dealer needs to add the selling details along with the owner's information.

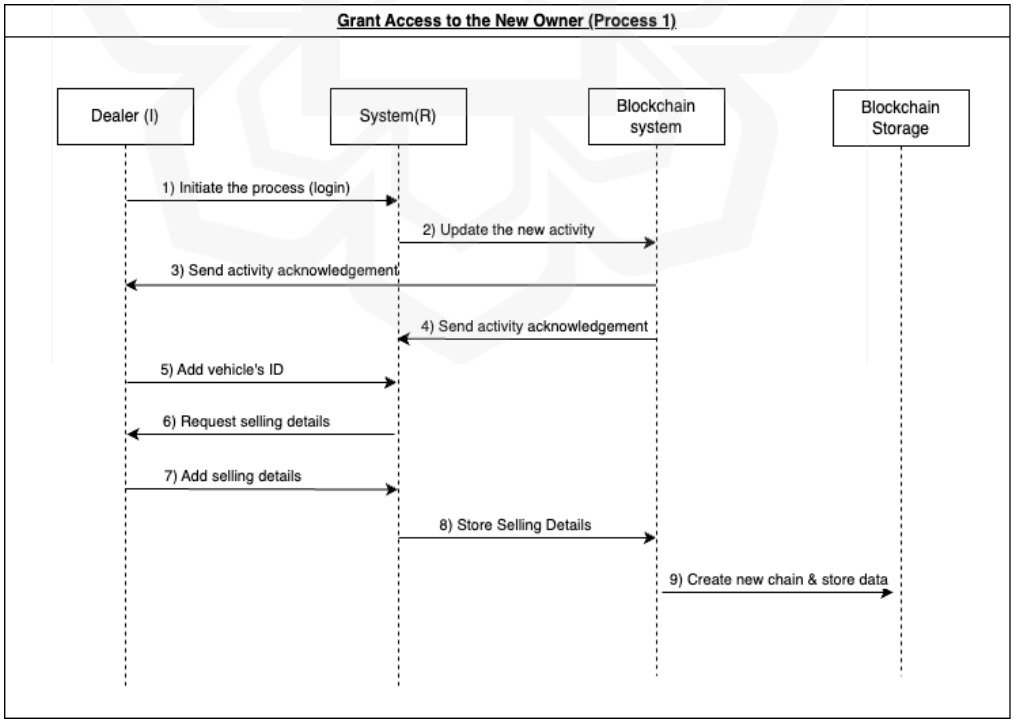


Figure 6 Sequence Diagram to Grant Access to the New Owner

Upon confirming the completeness and compliance of the provided details, the system securely stores the new data in the blockchain as a distinct block in the chain. This process ensures a seamless transition of ownership, incorporating authentication measures and blockchain technology to safeguard the integrity of the transaction and maintain a transparent record.

3.3.6 Analysis

During the framework design and communication protocol creation, a dual approach to design analysis is undertaken which are formal and informal analysis. Formal analysis is facilitated by the Scyther Tool to examine the design for security and efficiency. In parallel, informal analysis, which is a non-scientific yet iterative process, is carried out. This process involves continuous brainstorming, evaluation, and refinement to ensure that the framework and protocol evolve dynamically for optimal performance and effectiveness. In detail, the framework and protocol will undergo multiple discussions, assessments, edits, and improvements to verify whether the design aligns with the identified security requirements.

3.3.6.1 Scyther Tools

The designed communication protocol is then tested by a formal analysis using the Scyther Tool to identify if any threats could exploit communication between users. Emphasising the importance of ensuring both the correctness of the protocol and the safety and security

of the communication, this analysis was crucial in verifying that the proposed protocol is robust and resilient against potential attacks.

Scyther implements the Dolev-Yao model where an adversary has full control over the network that allows them to intercept, modify, or inject messages but not break cryptographic primitives. This model provides a rigorous security evaluation to ensure that the protocol can withstand various real-world attack scenarios. It systematically checks the protocol against various potential attacks to ensure its robustness under different threat scenarios.

In the Scyther tool, the authentication properties are verified through secret, agreement, aliveness and synchronisation properties. Secret property is applied to check and ensure that certain information is not revealed to an adversary, even though the communication is happening over an untrusted network. Aliveness verifies the authentication of communication partners that execute the events. Synchronisation will test for a stronger authentication requirement that verifies not only the communication partners but also the sequence of exchanged messages (Cremers et al., 1998). The last property is agreement which is tested to verify each data that is being exchanged between the agents.

By testing the protocol against these types of threats, Scyther was essential in verifying that the designed protocol could withstand such attacks. This analysis confirmed that the protocol meets the necessary security requirements, ensuring safe and secure communication between stakeholders in the vehicle maintenance service records ecosystem.

3.3.6.2 Testing Environments

The Scyther Tool demands several settings to be configured before protocol analysis. These settings involve verification parameters and advanced parameters. Verification parameters include essential elements such as the maximum number of runs required for protocol analysis. The specific number of runs varies based on the number of communications within the protocol. For instance, if the protocol involves seven communications, the maximum number of runs must be set to at least eight to ensure comprehensive safety against potential attacks across all communications.

Once the test is run, the results will be displayed as shown in Table 6. There are three types of results which are failed, ok and ok (verified). In the case of the results showing the status 'failed', it shows that during the testing process, the communication is prompted to have at least one attack which means the communication is not secured. For example, if the communication is tested to check its confidentiality, the result of one attack means the communication is prompt to have confidentiality issues. If the results show 'Ok' only, the communication is free from any attack within bounds. Lastly, the most secure communication is when the results show 'Ok' with verified notes where there is zero possibility of attack in that communication. This means the protocol has been tested in the maximum number of runs, and it shows that there is no possible attack on the communication protocol.

Table 6: Type of Testing Result & Descriptions

Status	Comments
Failed (red)	At least 1 attack

Ok (dark green)	No attacks within bound
Ok (light green)	No attacks

3.3.6.3 Security Concerns

The security requirements that have been highlighted in Section 3.3.2 are tested using the Scyther tool. Testing in the Scyther tool is run using claim events. Thus, the highlighted security requirements are integrated with the claim events in the Scyther tool. This section provides an in-depth explanation of the claim events and their comparison with the security requirements listed. The summary of the claim event and its properties is shown in Table 7.

The first claim event is 'secret' which means secrecy which is the same as confidentiality. This claim indicates that certain information must remain undisclosed to the unauthorised user, even when being communicated over an unsafe network.

The second claim event is 'ni-agree' where the testing revolves around achieving agreement as a security property. There are two types of agreement which are injective agreement (i-agree) and non-injective agreement (ni-agree). In this research, non-injective agreement is tested to satisfy the security requirements of providing data authentication.

The third claim is 'ni-synch' which means synchronisation. Synchronisation is divided into two types as well which are injective synchronisation (i-synch) and non-injective synchronisation (ni-synch). Non-injective synchronisation is applied in this study as a testing type to satisfy the security requirements of data and user authentication.

The fourth claim event is ‘alive’ which means aliveness. Aliveness is specifically focusing on the security requirements of the integrity of data and users. In this context, the objective is to ensure that the communication is occurring in real-time. Ensuring aliveness contributes to maintaining the integrity of users and data by confirming that they are not only present but also in a valid and unchanged state.

Table 7: Comparison of the Claim Events, Security Properties and Security Requirements

Claim Event	Security Properties	Security requirements
Secret	Secrecy	Confidentiality
Ni-Agree	Agreement	Data Authentication
Ni-Synch	Synchronisation	User & data Authentication
Alive	Aliveness	User & Data Integrity

CHAPTER FOUR

RESULTS & ANALYSIS

4.1 PROPOSED SOLUTION

4.1.1 Introduction

This chapter carries a thorough examination of the research results, building upon the highlighted goals as mentioned in the previous chapter where the challenge of maintaining accurate vehicle maintenance service records through the establishment of a reliable and secure record-keeping system has been addressed.

To initiate our discussion, we present a list of stakeholders in section 4.1.2 and their respective roles in section 4.1.3. It serves as a foundational resource for assessing the related security measures that need to be taken into consideration.

Next, section 4.1.4 highlighted the contribution of stakeholder in the secure maintenance record management to see their roles and help in maintaining the security and safety of vehicle maintenance service records.

Moving forward, section 4.1.5 elaborates on the frameworks created for two distinct categories which are scheduled vehicle maintenance service records and repair vehicle maintenance service records. This thoughtful approach recognises the varied needs in

vehicle maintenance service records, ensuring a tailored framework for both scheduled maintenance and repairs.

In section 4.1.6, we explore the preliminary process of vehicle maintenance service records frameworks which is divided into three parts. The parts are the initialisation phase, granting access to users, and revoking access from users. These phases are needed in conjunction with the framework and protocol discussions, emphasising the importance of each step in ensuring a secure and efficient system.

Section 4.1.7 focused on a detailed sequence diagram, offering a visual representation of the communication involved in granting access to the new user. This segment provides a deeper understanding of the communication happening within the proposed system.

Lastly, section 4.1.8 provides a comprehensive explanation of the proposed protocol. This section explores the details of the protocol's construction, carefully crafted based on the preceding sequence diagram. Through an examination, this part clarifies the functionalities and features of the protocol, offering a comprehensive overview of its design and implementation.

4.1.2 Stakeholder List

Based on the comparison of stakeholders mentioned in the existing research highlighted in Section 3.3.1, seven main stakeholders that play major roles in vehicle maintenance service records are identified as shown in Figure 7. They are the vehicle manufacturers, dealers, vehicle owners (including first- and second-hand owners), independent workshops,

technology teams which are the teams that manage software updates, insurance companies, potential buyers of the vehicle and the legislators. The role of the stakeholders is considered in examining the security requirements needed in designing the framework as well as protocol construction.

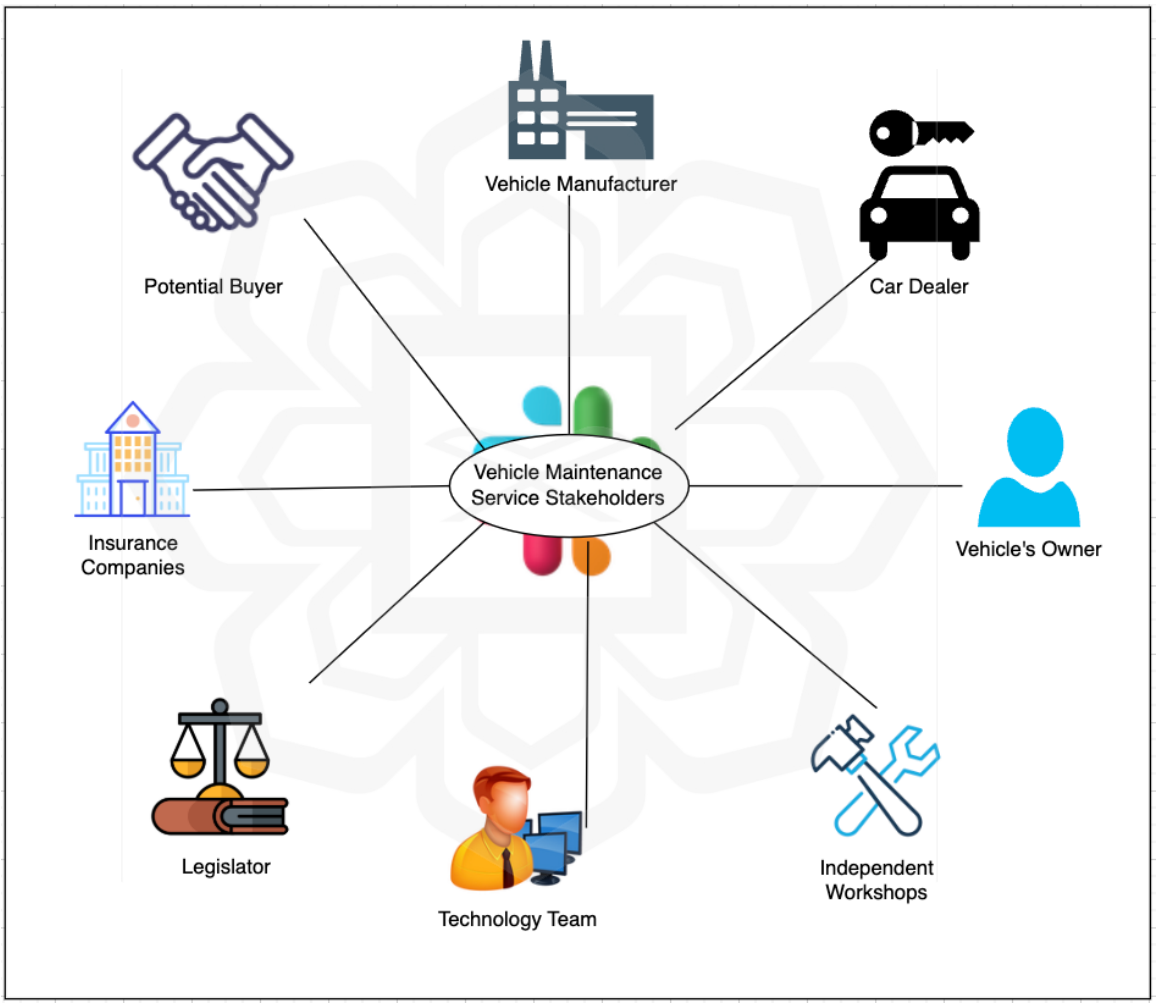


Figure 7 List of Stakeholders for Vehicle Maintenance Service Records

4.1.3 Stakeholder Role

In this section, the roles of each stakeholder that has been identified above are explained in detail. There are mainly seven important stakeholders whose roles are important in the vehicle maintenance service records management. Their roles are a source to identify the security measures that need to be considered in designing the secure solution in this research activity.

4.1.3.1 Vehicle Manufacturers

The vehicle life cycle begins when the manufacturers start to design, manufacture, assemble and distribute it. As vehicle manufacturers are responsible for the early life of vehicles, manufacturers are mainly responsible for recording the new vehicles with their complete details such as parts information, software details, and usage guidelines.

Their key responsibilities include providing initial data by uploading critical vehicle information such as the vehicle identification number (VIN), serial numbers, software versions, and usage guidelines directly to the blockchain. This data forms the genesis block as a trusted starting point for all subsequent records. The other key responsibility of manufacturers is to ensure the integrity of data by recording initial vehicle specifications on the blockchain as a guarantee that the information is immutable and cannot be altered fraudulently.

Manufacturers act as trusted nodes in the consortium blockchain, ensuring that all new vehicle data added to the system is validated and accurate. Their contributions prevent inconsistencies that could arise from incorrect or missing baseline data.

4.1.3.2 Car Dealers

Car dealers play a vital role as intermediaries between vehicle manufacturers and owners. Their responsibilities extend beyond sales to include the management of maintenance services in ensuring that vehicle-related data remains accurate and up-to-date throughout the ownership lifecycle.

One of their key functions is vehicle registration, where dealers validate and upload initial ownership records onto the blockchain once a vehicle is sold. This procedure creates a reliable and verifiable record of ownership, which serves as a key foundation for future maintenance and service updates.

Additionally, post-sale consultants work within dealerships to provide ongoing support to vehicle owners. They provide assistance to manage maintenance schedules, submit warranty claims, and ensure that updates such as service details and part replacements are accurately recorded on the blockchain. This role helps to streamline the maintenance process to ensure that vehicle owners remain informed and compliant with service requirements.

Another significant responsibility of dealerships is managing the warranty for the repairs that are related to the warranty and performed under the dealership's oversight. These repairs are securely logged into the blockchain to maintain traceability and accountability. By recording each repair, dealerships ensure that the service history is tamper-proof, providing stakeholders such as manufacturers, insurers, and future buyers the confidence in the vehicle's condition and maintenance integrity.

In the context of blockchain technology, car dealers act as data contributors who upload verified ownership records, warranty claims, and service updates. Their involvement guarantees that all information stored on the blockchain is accurate, immutable, and traceable. This not only enhances the transparency of data but also ensures the reliability of vehicle maintenance service records across the lifecycle of the vehicle.

4.1.3.3 Potential Buyers

The next stakeholders that are involved are potential buyers. There are two types of potential buyers which are the individuals who are interested in buying new cars and the individuals who aim to buy used vehicles.

Potential buyers rely heavily on accurate and tamper-proof maintenance records before they decide to buy the vehicle. They access the vehicle's maintenance history stored on the blockchain to verify repair records, part replacements, and past issues. This transparency allows buyers to ensure that a vehicle's condition aligns with its recorded history to foster trust during resale transactions. In the blockchain ecosystem, potential buyers act as temporary record viewers as well as leveraging blockchain immutability to confirm the authenticity of maintenance data. This approach addresses common concerns

such as fraudulent odometer readings or counterfeit maintenance reports, providing buyers with confidence in the data they access.

4.1.3.4 Vehicle Owners

There are two types of vehicle owners which are the individuals who own new vehicles and the individuals who own used vehicles. They are responsible for maintaining their vehicles to make sure that their vehicles are always in good condition for them to use or even to re-sell. They authorise repair shops or service providers to update maintenance data on the blockchain to ensure that all repairs and component replacements are accurately logged. Owners monitor their blockchain-verified service history to track maintenance activities and warranty coverage. These tamper-proof records enhance the resale value of their vehicles by providing transparent and credible maintenance histories. Within the blockchain system, vehicle owners act as authorised participants who can view but not alter records by maintaining transparency while preventing unauthorised modifications to historical data.

4.1.3.5 Repair Shops

The next stakeholder is repair shops; these are divided into three categories. They are the dealership (car dealers), as well as independent workshops and speciality shops that specialise in specific vehicle brands or parts of vehicles. Dealerships are the main option to get maintenance service because of the warranty. They are the industry's high-end shops, with mechanics trained by the manufacturers. Since they are also selling automobiles and parts, they provide a comprehensive service.

However, independent workshops are also considered as the most preferred place to get maintenance service especially if the vehicle's warranty has expired. It is because they are more reachable as they are more in number than the dealership. Moreover, the charge of their service is cheaper than the dealer. That becomes the reason why they are preferable to go to especially once the warranty of the vehicles has expired. The last category is speciality repair shops that provide special services focusing on specific brands and parts. These shops are the go-to shops for some vehicle owners if their vehicle requires specific expertise on specific repair jobs.

Repair shops are vital contributors to the dynamic updates of vehicle maintenance service records. After performing maintenance or repairs, they securely upload service details to the blockchain to preserve the integrity of the records. Spare parts shops then contribute to the process by verifying that only genuine components are recorded in the system. This helps to reduce the risk of counterfeit parts being introduced.

Repair shops also perform real-time diagnostics using tools like ECUs to upload verified data to the blockchain for traceability. As trusted data updaters, repair shops ensure that every service entry is validated, immutable, and traceable to significantly reduce the chances of fraudulent maintenance claims or falsified reports.

4.1.3.6 Technology Teams

Another stakeholder involved in vehicle maintenance service records is the technology team that handles software maintenance such as software updates and solving any errors or problems related to software. This involves applying the most recent developments in

software technology to maximise vehicle performance, boost productivity, and offer a better user experience. They are the stakeholders who are required to respond rapidly if there are any software-related issues during the vehicle's lifecycle.

These teams also provide real-time vehicle condition data, collected from ECUs and onboard diagnostic tools, which is then uploaded to the blockchain for accurate and transparent records. Any software-related issues or updates are securely logged to ensure accountability.

In the blockchain ecosystem, technology teams act as data validators, contributing real-time diagnostic information and software updates that uphold the integrity and accuracy of dynamic records.

4.1.3.7 Insurance Company

As vehicle maintenance service records stakeholders, insurance companies provide financial protection for the vehicle from possible hazards in the future. They are the parties who handle the process of compensating the policyholder by following the conditions that have been agreed upon with the vehicle owner. They are especially needed when maintenance is required due to accidents.

Insurance companies rely on accurate maintenance records to process claims and assess vehicle risks effectively. Blockchain-verified records are used to confirm that maintenance services were performed as claimed. This is important to reduce fraudulent claims. Other than that, historical records also allow insurers to evaluate the vehicle's condition. By accessing blockchain-verified data, insurers act as data verifiers to ensure transparency and accuracy in their processes while minimizing fraud in the insurance ecosystem.

4.1.3.8 Legislators

As stakeholders in vehicle maintenance service records, legislators provide crucial regulatory oversight to ensure that vehicle maintenance service records systems comply with legal and industry standards. They play an indirect but essential role in developing regulations for data protection, privacy, and system compliance. The role of the legislator is to enforce standardised formats for maintenance records to maintain interoperability among stakeholders. They also establish consumer protection laws to safeguard vehicle owners and buyers from data manipulation or fraudulent records.

In the blockchain framework, legislators contribute indirectly by defining policies that regulate data access, storage security, and record immutability as a part of ensuring that the framework aligns with industry regulations and legal requirements.

4.1.4 Stakeholder Contributions to Secure Maintenance Record Management

In vehicle maintenance service records management, stakeholders play a crucial role in maintaining the accuracy, integrity, and availability of data while ensuring confidentiality and non-repudiation. Each stakeholder contributes to securing vehicle maintenance service records in a way of generating, verifying, or accessing data within the ecosystem. Understanding their security responsibilities is essential to designing a secure framework and communication protocol that prevents unauthorised modifications, fraudulent claims, and data breaches.

This section outlines how each stakeholder influences the security of maintenance records, particularly in terms of data validation, access control, and record authenticity. By integrating security-focused roles into the stakeholder analysis, this research ensures that

vehicle maintenance service records are tamper-proof, reliable, and accessible to authorised entities only.

Stakeholders also contribute to data validation. Workshops or technology teams can validate maintenance records in real-time using diagnostic tools, such as ECU data, which prevents any error from manual data entry or unauthorised modifications. Furthermore, including all relevant stakeholders creates a comprehensive audit trail for each record. If a record is questioned, the system can trace it back to the responsible entity whether it is the repair shop, manufacturer, or another stakeholder.

In addition, stakeholders play a vital role in ensuring the availability of vehicle maintenance service records. By identifying stakeholders, the system can assign appropriate access rights based on their roles. For example, vehicle owners should have read-only access to their vehicle records, repair shops can update records but cannot delete or overwrite historical data, and insurers can access records to validate claims but cannot alter them. This structured access control prevents misuse of data while ensuring that records are available to authorised parties.

A decentralised data storage system, such as a consortium blockchain ensures data is stored across multiple locations, improving fault tolerance and minimizing the risk of downtime. If one node, like a workshop's server, fails, the system can still retrieve data from other nodes, ensuring the continuous availability of the records. Stakeholders also create a collaborative environment in which data accessibility is guaranteed by mutual reliance. For instance, when a vehicle owner visits a repair shop, the shop can easily retrieve the vehicle’s previous maintenance history from the blockchain to provide accurate service.

The stakeholders that have been identified play a crucial role in establishing a safe environment where vehicle maintenance record access is strictly controlled. For example, manufacturers upload initial vehicle details, repair shops update records after services, and insurers access records for claims verification. Additionally, stakeholders such as blockchain nodes ensure that once a record is added, it cannot be tampered with to preserve the integrity of data.

While the secure framework ensures the structure of the system is robust, secure communication ensures that data exchanges between stakeholders are protected. For instance, when a repair shop updates a record, the data is transmitted through an encrypted channel to the blockchain network. This will help to prevent any data tampering during transmission. Similarly, insurers validate maintenance data using secure authentication mechanisms to verify the source of the information. Thus, the secure framework ensures data integrity and controlled access, while secure communication ensures the safe exchange of data, preventing unauthorised access or data breaches.

Some stakeholders are relevant to the vehicle maintenance ecosystem but not directly reflected in the framework because their roles do not involve direct interaction in managing vehicle maintenance service records. Their involvement is more indirect, such as providing regulatory oversight, supporting backend processes, or influencing policies rather than actively contributing to the maintenance record transactions. For example, legislators establish data protection regulations but do not directly participate in record validation or updates. Similarly, potential buyers rely on blockchain-verified records for decision-making but do not contribute to the data entry or approval process. Thus, the framework primarily includes stakeholders who actively generate, validate, and manage vehicle maintenance records within the blockchain ecosystem.

Stakeholders play a crucial role in digital forensics, which relies on accurate and traceable data to investigate security incidents, identify malicious activities, or resolve

disputes. Their involvement enhances traceability by ensuring that every interaction with the system is logged, creating a comprehensive audit trail. For instance, when a repair shop updates a record, the system records the time, date, and source of the update. Using blockchain's immutable ledger, these changes are permanently logged, aiding forensic analysis in detecting unauthorised modifications or anomalies.

Stakeholders also support data integrity by providing accurate and reliable records. For example, in cases where a vehicle owner disputes a service claim, records verified by manufacturers or repair shops can be used as evidence. Moreover, stakeholders facilitate accountability, as the system can trace actions back to specific entities. If a record is found to be falsified, the responsible stakeholder, such as an insurer or repair shop, can be identified.

Additionally, stakeholders enable secure evidence sharing, ensuring that maintenance records or diagnostic data are securely transmitted to investigators. This approach preserves the chain of custody and upholds the integrity of the evidence, making stakeholders integral to the success of digital forensic processes.

By thoroughly identifying stakeholders and defining their roles, this research addresses potential issues of data inaccuracy and unavailability. Without proper stakeholder identification, the system would lack accountability and fail to deliver a reliable and transparent vehicle maintenance service records management solution. Furthermore, stakeholders help to build a safe framework that protects data through secure communication while also enabling traceability and responsibility for digital forensics. The following Table 8 presents an overview of stakeholder responsibilities concerning security requirements.

Table 8: Summary of Stakeholders and Their Roles

Stakeholders	Roles	Relation to Framework	Impact on the Security Requirements
Vehicle Manufacturers	Provide initial vehicle data, including specifications and part serial numbers.	Generate foundational records for maintenance history.	Contribute to data integrity and availability by providing accurate initial data.
Dealers (Including Post-Sale Consultants)	Record initial ownership details upon vehicle sale. Assist owners in managing maintenance schedules and warranty claims.	Upload verified ownership and warranty data to the blockchain for traceability.	Provide data integrity and authentications of service data and updates and prevent fraudulent warranty claims.
Potential Buyers	Make informed purchasing decisions by accessing accurate maintenance records.	Temporary access to vehicle maintenance service records that are stored on the blockchain to verify repair records, part replacements, and past issues.	Ensures transparency and prevents misinformation (integrity) in resale transactions.

Vehicle Owners	Authorise service updates to be recorded on the blockchain. Access vehicle maintenance service records to monitor repairs and part replacements.	Ensure maintenance records reflect actual performed services and enhance resale value. Promote transparency and trust through verified record access.	Non-repudiation guarantees that once a maintenance record is added, the responsible party (e.g., repair shop, dealer) cannot deny or alter the service performed to ensure the availability and integrity of data
Repair Shops	Perform maintenance and repairs, then upload service details. Validate and record the use of genuine spare parts.	Ensure records reflect accurate, real-time maintenance updates.	Provide integrity by preventing falsified records and the use of counterfeit parts.
Technology Teams	Apply software updates and resolve software-related issues.	Support secure communication by ensuring reliable and updated systems.	Ensures secure communication between stakeholders.
Insurance Company	Verify maintenance histories for claim processing.	Ensure that claim decisions are based on tamper-proof records.	Provide integrity & non-repudiation to prevent financial losses due to false

			maintenance claims.
Legislators	Define data protection regulations and compliance frameworks.	Ensure the system aligns with industry standards and protects user privacy.	Ensures compliance with legal requirements to enhance trust and accountability across the ecosystem.

4.1.5 Proposed Framework

In this section, the details of the proposed framework are discussed. The framework includes all the main stakeholders listed in Section 4. There are two different frameworks based on two different maintenance service use cases which are Scheduled Service Framework and Repair Service Framework.

The proposed framework integrates a consortium blockchain model to enhance security, transparency, and reliability in vehicle maintenance service records. This approach ensures that only authorised stakeholders such as manufacturers, repair shops, insurers, and vehicle owners can validate and update maintenance records. By implementing a decentralised yet controlled environment, the framework prevents unauthorised modifications while maintaining availability and accessibility for relevant stakeholders.

Unlike public blockchains that allow unrestricted participation, the consortium model restricts access to verified entities to reduce computational overhead and improve efficiency. This selective participation enhances trust and accountability within the vehicle

maintenance ecosystem by ensuring that all service records, part replacements, and warranty claims are securely stored, immutably recorded, and verifiable. The integration of blockchain into the framework mitigates risks related to fraud, counterfeit parts, and unauthorised record alterations, creating a tamper-proof system for managing vehicle maintenance data.

Within the vehicle maintenance ecosystem, various stakeholders operate individual data management systems. For instance, dealership networks may utilize private blockchains to handle customer transactions, service records, and staff authorisations, while repair shops may maintain separate systems for inventory tracking, technician activities, and service updates. To enable seamless data sharing and verification, these private blockchains are interconnected with a larger, shared consortium blockchain, which acts as a trusted ledger for maintenance service records across multiple entities.

By linking private and consortium blockchains, this architecture ensures that internal business operations remain protected, while cross-entity maintenance data remains accurate, consistent, and auditable. This hybrid model effectively balances data security and operational efficiency, reinforcing compliance, accountability, and long-term reliability in vehicle maintenance record management.

4.1.5.1 Scheduled Service

During the manufacturing of the vehicle, the manufacturer will indicate the scheduled maintenance services that the vehicle will require, as well as ideas on how to repair some damage and a complete list of services required. There are times when the owner must

return the car to the service centre to have maintenance performed, such as when a specific mileage is reached. However, if the vehicle is not used regularly, it will require maintenance after a given amount of time. Currently, the information is given to the owner in the form of a manual book or a next service post-notes which is usually given upon the completion of maintenance service.

In this research, instead of relying on the manual reminder, the information is proposed to be kept in the system so that when the vehicle is required to receive maintenance service, the system will send the notification to the owner. Figure 8 demonstrates the proposed framework of scheduled maintenance service.

First, when the vehicle assembly is finished and ready to be sold, the manufacturer will upload the vehicle information, including parts and maintenance details, as well as warranty information, to the cloud, which will then be shared with the owner once the car gets purchased. Then, once the car has been sold and utilised, a notification or alert message is delivered through the system to the vehicle owner when the vehicle requires maintenance work. Next, before the maintenance service is performed, the system will send a request to the diagnostic tool to get the vehicle's present status from the ECU. The extracted data is stored as a vehicle condition record before maintenance service.

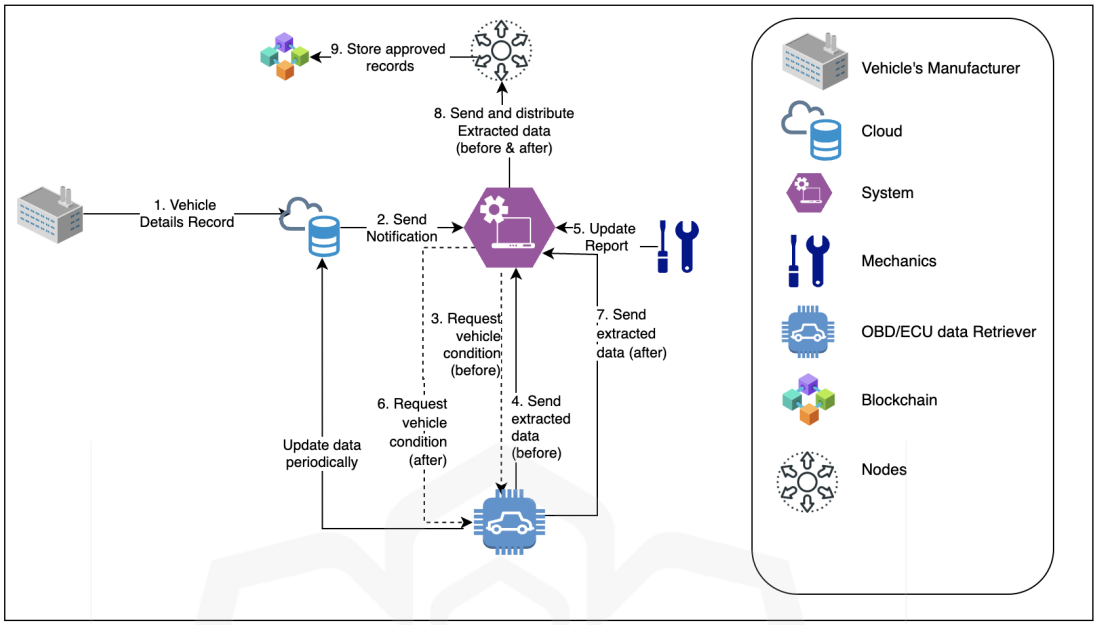


Figure 8 Framework for Scheduled Maintenance Service

Upon the completion of the repair service, the technician must update the report in the system, as illustrated in Step 5 of Figure 8. After the maintenance service is done, the data from the car is extracted once more to obtain the vehicle condition record.

For the next step, the record of data that has been extracted before and after maintenance is sent to the participating nodes in the blockchain. The nodes include the stakeholders that have been discussed in the previous section

as members of the consortium blockchain. Here, the nodes will check whether the vehicle condition report before and after maintenance is valid to be approved. If more than 80 per cent of the nodes give their approval, then the record is stored in the blockchain. A new block in the blockchain is produced to keep each document that has been approved by the nodes. The record is saved together with the timestamp and hash value, as well as the previous block's hash value. This will generate a blockchain of records that is immune to data manipulation.

4.1.5.2 Repair Service

Apart from scheduled service, a framework for maintenance service when there is damage or repair needed is also considered as shown in Figure 9. There are a few situations which would require the vehicle to receive a repair maintenance service. One such situation is when there is an in-vehicle notification that shows a problem in any part of the vehicle. Other than that, repair maintenance service would also take place when there is any physical damage that is encountered by the vehicle through accidents.

In the framework, an on-board diagnostic (OBD) tool will periodically retrieve the vehicle's condition from the ECU and save it in the cloud for future reference. The procedure is repeated once a week or at a predetermined mileage established by the manufacturer.

When there is any damage detected, the system will automatically request the vehicle’s condition record from the ECU. The data extracted is stored in the cloud. After the repair service, the mechanic is required to update the maintenance report in the system. When there is an update from the mechanic, data from the ECU is extracted to get the latest vehicle condition.

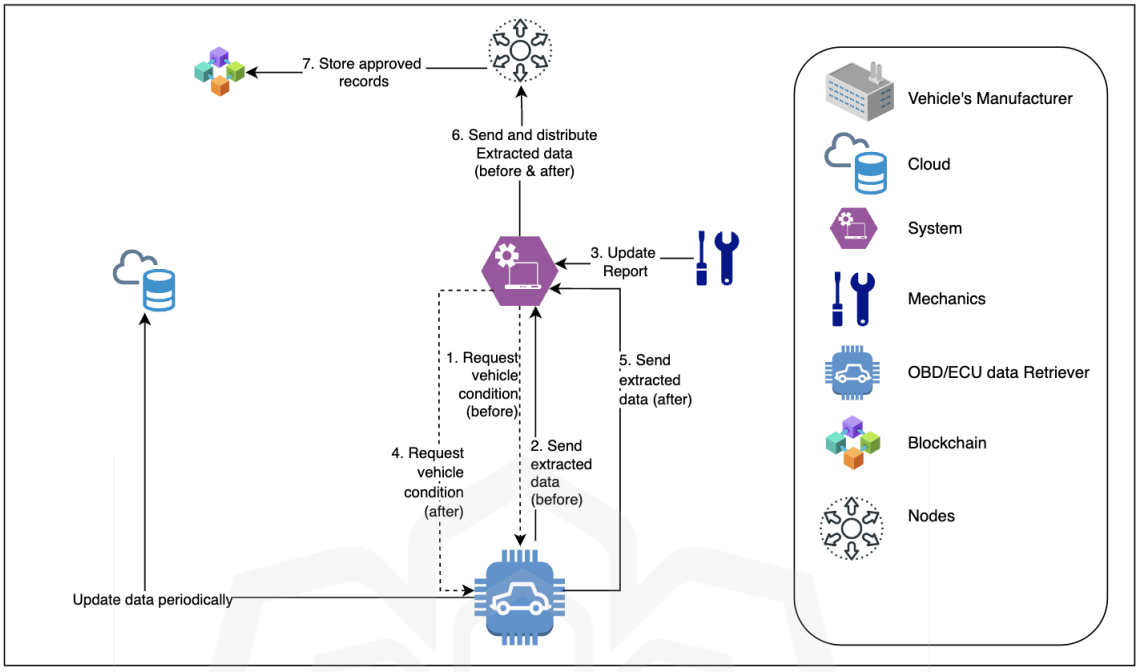


Figure 9 Framework for Repair Maintenance Service

The three records will then be distributed to the participating nodes to be stored on the blockchain. The three records are vehicle condition records extracted from the ECU before getting maintenance service, vehicle maintenance service records retrieved from the ECU following repair service, and the report that is updated by the maintenance service provider.

To figure out whether the mistakes have been resolved, the current state is compared to the previous condition that contained the problem. The mechanics' report will also be checked to verify that it matches the records collected from the ECU. The participating nodes of the consortium blockchain will complete this task. Following the verification process, a new block is produced in the blockchain to hold the records along with the timestamp, new hash value, and previous block hash value.

4.1.5.3 Comparison of Scheduled vs. Repair Services

To address the diverse needs of vehicle maintenance service records, this research presents two distinct frameworks which are scheduled maintenance services and repair maintenance services. While both frameworks leverage consortium blockchain for transparency and security, their processes differ significantly based on the nature of the service. Table 9 highlights a clear distinction between their design and operational focus.

Table 9: Comparison of Scheduled and Repair Maintenance Services

Aspects	Scheduled Maintenance Services	Repair Maintenance Services
Primary Purpose	Regularly scheduled maintenance to prevent vehicle issues.	Address unexpected or ad-hoc repairs and breakdowns.
Initial Step	Based on manufacturer-recommended schedules (e.g., mileage, time).	Triggered by user report or diagnostic alert.
Approval and Storage	Data verified by manufacturers and stored in blockchain as preventive service history.	Data verified by repair shops and stored as reactive repair records.
Data Interaction	Interaction initiated by vehicle owners or reminders from the system.	Interaction initiated by repair shops after inspection.

Mechanics Involvement	Standardised procedures; minimal deviation across vehicles.	Tailored procedures; dependent on vehicle-specific needs.
Data Extraction	Extracted from ECU or onboard systems during regular checkups.	Extracted from diagnostic tools during issue resolution.
Blockchain Usage	Focus on transparency and long-term traceability for routine maintenance.	Focus on accuracy and validation of emergency repairs.
Periodic Updates	Requires regular updates per maintenance schedule.	Requires updates only when repairs occur.
Stakeholders	Manufacturers, dealers, owners, and insurance companies.	Repair shops, owners, and insurance companies.

4.1.6 Preliminary Process

This segment focuses on the initial stages of ensuring the secure management of vehicle maintenance service records, encompassing three important phases which are initialisation, access provisioning for new users, and access revocation. The initialisation phase involves the registration of new vehicles, orchestrated by the vehicle's manufacturer.

Upon completion of the manufacturing process, the manufacturer assumes responsibility for registering the vehicle and uploading its metadata, encompassing the vehicle identification number, manufacturing date, and serial numbers of components. This

metadata is then securely stored in the blockchain as a new block for the specific vehicle blockchain.

Moving forward, the subsequent phase involves the facilitation of access for new users, classified into two categories: temporary users such as potential buyers, independent workshops, and insurance companies, and permanent users, including the dealership, vehicle owner (granted access upon purchase), and technology teams.

The last phase centres on the process of revoking access for users previously granted entry into the system there are two types of users which are permanent users, such as the vehicle owner, whose access is terminated upon vehicle sale, and temporary users, where access revocation is crucial to adherence to predefined time constraints. For instance, temporary users should only retain access for the necessary period dictated by their specific requirements. The summary of the preliminary process is shown in Figure 10.

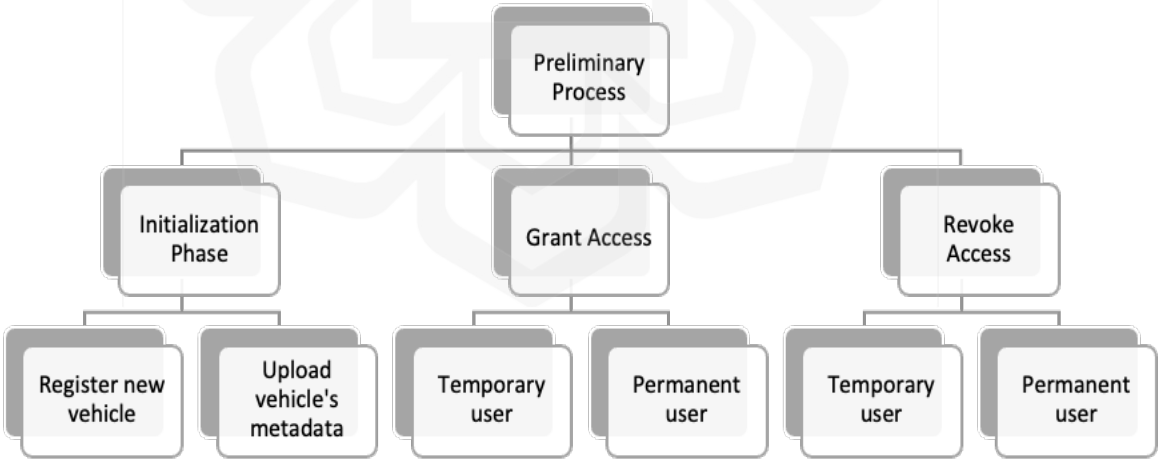


Figure 10 Summary of Preliminary Process

4.1.7 Proposed Protocol

4.1.7.1 Protocol Description

Building on the insights gained from both framework design and the comprehensive threat analysis, the research proceeded to produce a secure communication protocol. As stated in 4.1.5, the framework requires some preliminary actions which are the initialisation phase, grant access phase and revoke access phase.

The secure communication protocol proposed in this study focuses on the grant access process, enabling new vehicle owners to gain authorised access to vehicle maintenance service records. By implementing encryption and authentication mechanisms, the protocol ensures the secure transmission of sensitive data, such as user credentials and vehicle ownership details, among stakeholders like dealers, web systems, and blockchain nodes. This approach prevents unauthorised interception or tampering during the access provisioning process.

Although the grant access phase is the primary focus of this research, it establishes a foundation for extending secure communication to other critical processes, such as data updates and maintenance verification, which will be considered in future work. Designed with the stringent requirements of digital forensics in mind, the protocol ensures the integrity and security of data transmission. By facilitating seamless and secure communication among stakeholders, the proposed protocol aligns with best practices for maintaining trust, transparency, and traceability within the vehicle maintenance service records ecosystem.

The secure framework and grant access protocol together enhance traceability and accountability within the system. Every action related to granting access, such as updates or transmissions, is logged on the blockchain with a timestamp, entity details, and transaction records. These immutable logs create a comprehensive audit trail that supports digital forensics by allowing investigators to trace back unauthorised access attempts, changes to permissions, or data-related anomalies. This level of traceability ensures that stakeholders are held accountable for their actions, and any malicious activity can be quickly identified and addressed.

Embracing an iterative design approach, the protocol undergoes multiple rounds of refinement and testing. This iterative cycle allows for continuous improvements based on real-world scenarios, emerging security threats, and the dynamic technological landscape.

In essence, the journey from framework design to the development of a secure communication protocol represents a meticulous and strategic progression, where each step is imbued with the overarching commitment to fortify the security, integrity, and forensic capabilities of vehicle maintenance service records. The proposed secure framework ensures the reliability and integrity of vehicle maintenance service records through blockchain's immutability and role-based access controls. The secure communication protocol that focuses on the grant access process is an important part of establishing a foundation for protecting sensitive data during critical interactions. Thus, the combination of these contributions will enhance digital forensic capabilities by enabling traceability, accountability, and tamper-proof data management.

4.1.7.2 Protocol Notation

A comprehensive overview of the protocol notation employed in this research is presented in Table 10 as a reference point for the communication protocol designed. There are three roles in this protocol which are car dealer, web system and blockchain system.

Table 10 List of Notations Used in Protocol

Notation	Description
CD	Car Dealer
WS	Web System
BCS	Blockchain system
ssk	Secured Session key
psk_x	Preshared Symmetric Key of x = cd, ws, bcs
pk_x	Public key of x = cd, ws
n_k	Secret nonce of k = cd, ws

4.1.7.3 Proposed Protocol

The protocol to grant access to the new owner of the vehicle is shown in Table 11. Upon completing the vehicle selling process, the dealer who is overseeing the buying process is responsible for requesting access for the new owner. This communication involves the dealer, web system and blockchain system.

Table 11 Proposed Protocol to Grant Access to the New Owner of Vehicle

1.	CD →WS	:	$\{M1\} \parallel psk_{(cd, ws)}$
			$M1 = n_{cd}, cd$
2.	WS → BCS	:	$\{M2\} \parallel psk_{(ws, bcs)}$
			$M2 = cd, n_{cd}, n_{ws}$
3.	BCS → CD	:	$\{M3\} \parallel psk_{(cd, bcs)}$
			$M3 = ws, ssk, n_{cd}, n_{ws}$
4.	BCS → WS	:	$\{M4\} \parallel psk_{(ws, bcs)}$
			$M4 = cd, ssk$
5.	CD →WS	:	$\{M5\} \parallel ssk$
			$M5 = cd, ws, bcs, n_{ws}$
6.	WS → CD	:	$\{M6\} \parallel pk_{cd}$
			$M6 = n_{cd}, n_{ws}, ws$
7.	CD →WS	:	$\{n_{cd}\} \parallel pk_{ws}$
8.	WS → BCS	:	$\{M7\} \parallel psk_{(ws, bcs)}$
			$M7 = cd, n_{cd}, n_{ws}$

Table 11 shows the secure communication protocol to grant access to the new owner of the vehicle and the details explanation on the communication are explained below:

1. The car dealer (CD) initiates the process of communicating with the web system (WS) by sending a secret nonce (n_{cd}) and identification of the car dealer (*cd*). The nonce (n_{cd}) is encrypted using the pre-shared symmetric key ($psk_{(cd, ws)}$) of the car dealer and web system.

2. The web system (WS) interacts with the blockchain system (BCS) to update that there has been an activity being initiated by a car dealer (CD). This involves sending the car dealer's identification (*cd*), the car dealer's secret nonce (n_{cd}), and the web system's secret nonce (n_{ws}). The message is encrypted using the pre-shared symmetric key ($|psk_{(cd, bcs)}$) of both the web system and the blockchain system.

3. The blockchain system (BCS) communicates with the car dealer (CD) by sending the acknowledgement of the initiated activity. The communication consists of the identification of the web system (*ws*), a secured session key(*ssk*), and the secret nonces of both the car dealer and the web system ($n_{cd,}\, n_{ws}$). This information is encrypted using the pre-shared symmetric key ($psk_{(cd, bcs)}$) shared between the car dealer and the blockchain system.

4. In parallel with communication number 3, the acknowledgement from the blockchain system (BCS) is sent to the web system (WS) as well. The acknowledgement communication consists of the identification of the car dealer (*cd*) and a secured session key (*ssk*). This information is encrypted using the pre-shared symmetric key ($psk_{(ws,\ bcs)}$) shared by the web system and blockchain system.

5. Car dealers (CD) communicate with the web system (WS) by sending an identification of all the roles involved which are car dealer (*cd*), web system

(*ws*) and blockchain system (*bcs*) together with the secret nonce of web system (n_{ws}). The message is encrypted using a secure session key (*ssk*) that has been generated and received from the blockchain system in the previous step.

6. Web system (WS) is then communicated with the car dealer (CD) by sending a message containing the secret nonce of the car dealer and web system ($n_{cd,}\, n_{ws}$) as well as the identification of the web system (*ws*). The message is encrypted using the public key of the car dealer (pk_{cd}).

7. Next, the car dealer (CD) communicates with web the system (WS) by sending the message containing a secret nonce of the car dealer (n_{cd}) that is encrypted using the public key of the web system (pk_{ws}).

8. Lastly, the web system (WS) interacts with the blockchain system (BCS). The message contains the car dealer's identification (*cd*), the car dealer's secret nonce, and the web system's secret nonce ($n_{cd,}\, n_{ws}$). The message is encrypted using the pre-shared symmetric key ($psk_{\,(ws,\ bcs)}$) of the web system and the blockchain system.

4.2 ANALYSIS

The protocol outlined in section 4.1.7.3 is tested involving a continual analysis that includes both informal and formal methodologies. The analysis starts by doing an informal assessment where a thorough examination is conducted to identify potential vulnerabilities and risks. Then, a threat model is built to list down the threats that may arise and accompanied by effective countermeasures to mitigate these potential risks.

Next, formal testing to test the security of the protocol's security is conducted by using the Scyther Tool. Scyther Tool is a specialised tool designed for security analysis. In this testing, the protocol's design is tested to ensure its resilience against potential threats and vulnerabilities. This dual approach, combining informal analysis and formal testing with the Scyther Tool, contributes to the comprehensive and robust security posture of the protocol.

4.2.1 Informal Analysis

Informal analysis is performed to evaluate the designed frameworks and protocols. It is to check whether the possible threats listed in Section 3.3.3 are covered and secured by the design of the proposed framework and protocol.

4.2.1.1 The Threat of Using Soft Copy Version and Its Solutions

The results of the threat modelling process undertaken for this study are explained in this part. The focus is on identifying and analysing potential threats, vulnerabilities, and associated risks within the system under consideration. This study utilised two primary threat modelling approaches which are the Threat, Vulnerability, and Risk Assessment (TVRA) and the STRIDE model. TVRA helped to systematically evaluate vulnerabilities and assess risks, while STRIDE served as a complementary model to categorise and understand the nature of each threat more deeply. This dual approach provides a more comprehensive understanding of the system’s security landscape by highlighting areas where improvements can be made. By categorising threats through both methods, this research aims to identify not only immediate risks but also long-term security weaknesses

that may affect the system. The analysis in this chapter is intended to underscore the importance of these findings in informing effective security measures.

The identified threats are compiled in a summary table that combines the insights from both TVRA and STRIDE. Table 12 presents each identified threat, the specific vulnerabilities it exploits, the assessed level of risk, and the mitigation measures recommended. The risk prioritization is identified based on the described rate as below:

- **High Impact:** Immediate mitigation is required (e.g., data integrity protection, strong authentication mechanisms).
- **Medium Impact:** Addressed through system resilience and monitoring.
- **Low Impact:** Can be mitigated as part of routine improvements.

Additionally, each threat is categorised according to the STRIDE model, providing further context on the nature of each security issue. For example, if a vulnerability is related to unauthorised data modification, it might be categorised under "Tampering" in STRIDE, while unauthorised access issues would fall under "Spoofing." This tabular overview helps visualise the security challenges within the system, making it clear which areas require prioritised attention and which mitigation strategies are most effective. Presenting the results in this format allows for a clearer, more organised interpretation of the threat landscape, making it easier to identify patterns and trends in vulnerabilities and associated risks.

Table 12 The Threats and Challenges of Keeping the Vehicle Maintenance Service Records and Its Mitigation

No	Threat Description	Vulnerability	Risk Assessment (Likelihood/ Impact)	Mitigation	STRIDE Category
1	Unauthorised login	Weak authentication	High	Two-factor authentication (2FA) with secure communication protocol	Spoofing
2	Unauthorised data modification	Weak data integrity	High	Encryption, data validation	Tampering
3	Records alteration	Store records in editable format	High	Implementation of consortium blockchain	Tampering
4	Falsified records update	Lack of verification of actual maintenance tasks	High	Extract data from ECU before and after service to validate data. Store data in the blockchain	Tampering
5	Unauthorised and unverified new data	Lack of verification of data authenticity and its sources	High	Each record can be updated only by an authorised user with a credential	Repudiation

6	Records deletion	Systems allow data deletion	High	Implementation of consortium blockchain	Repudiation
7	Data leak due to interception	Unencrypted data transmission	High	Encryption during transmission	Information Disclosure
8	Malicious actors inject false or manipulated data into a system	Insufficient integrity and authenticity checks on incoming data expose	High	Implementation of consortium blockchain and data authentication	Denial of Service
9	Impersonation enables unauthorised access to sensitive data	Lack of robust authentication mechanisms	High	Implementation of secure communication protocol	Elevation of Privilege

4.2.1.2 Evaluation of Security Requirements Compliance

To ensure that the proposed security framework effectively mitigates potential threats, an evaluation is conducted based on the security requirements of Confidentiality, Integrity, Availability, Authentication, and Non-repudiation. Each identified threat is analysed to determine whether the applied security controls sufficiently address the associated vulnerabilities. The compliance status is assessed to verify if the security requirements are met, ensuring that the vehicle maintenance service records remain secure, accurate, and tamper-resistant.

Table 13 below presents a structured assessment of the identified threats, their corresponding security requirements, implementing mitigation strategies, and compliance status. This evaluation helps validate the effectiveness of the security mechanisms in protecting vehicle maintenance service records against unauthorised access, data manipulation, and loss of integrity.

Table 13 Security Assessment of Threats, Mitigation Strategies, and Compliance Status for Vehicle Maintenance Service Records

No	Threat	Security Requirements	Mitigation	Compliance Status
1	Unauthorised login	Authentication, Non-repudiation	Two-factor authentication (2FA) with secure communication protocol	✓
2	Unauthorised data modification	Integrity, Authentication	Digital signatures, blockchain consensus validation	✓
3	Records alteration	Integrity, Non-Repudiation	Immutable blockchain storage, cryptographic hashing	✓
4	Falsified records update	Integrity, Non-Repudiation	Extract ECU data before & after service, verify against the blockchain	✓

5	Unauthorised and unverified new data	Integrity, Authentication	Multi-stakeholder validation, consensus-based approval	✓
6	Records deletion	Availability, Integrity	Tamper-proof blockchain storage, backup and recovery mechanisms	✓
7	Data leak due to interception	Confidentiality, Authentication	Secure encryption during data transmission	✓
8	Malicious actors inject false or manipulated data into a system	Integrity, Non-repudiation, Authentication	Digital signatures, smart contract-based validation, blockchain consensus	✓
9	Impersonation enables unauthorised access to sensitive data	Authentication, Confidentiality	Implementation of Secure Communication Protocol	✓

4.2.2 Formal Analysis

4.2.2.1 Testing Code

As mentioned above, the testing has been formally done using the Scyther Tool. The test focuses on the communication protocol to grant access to the new owner of the vehicle. The testing code is shown in Figure 11 below.

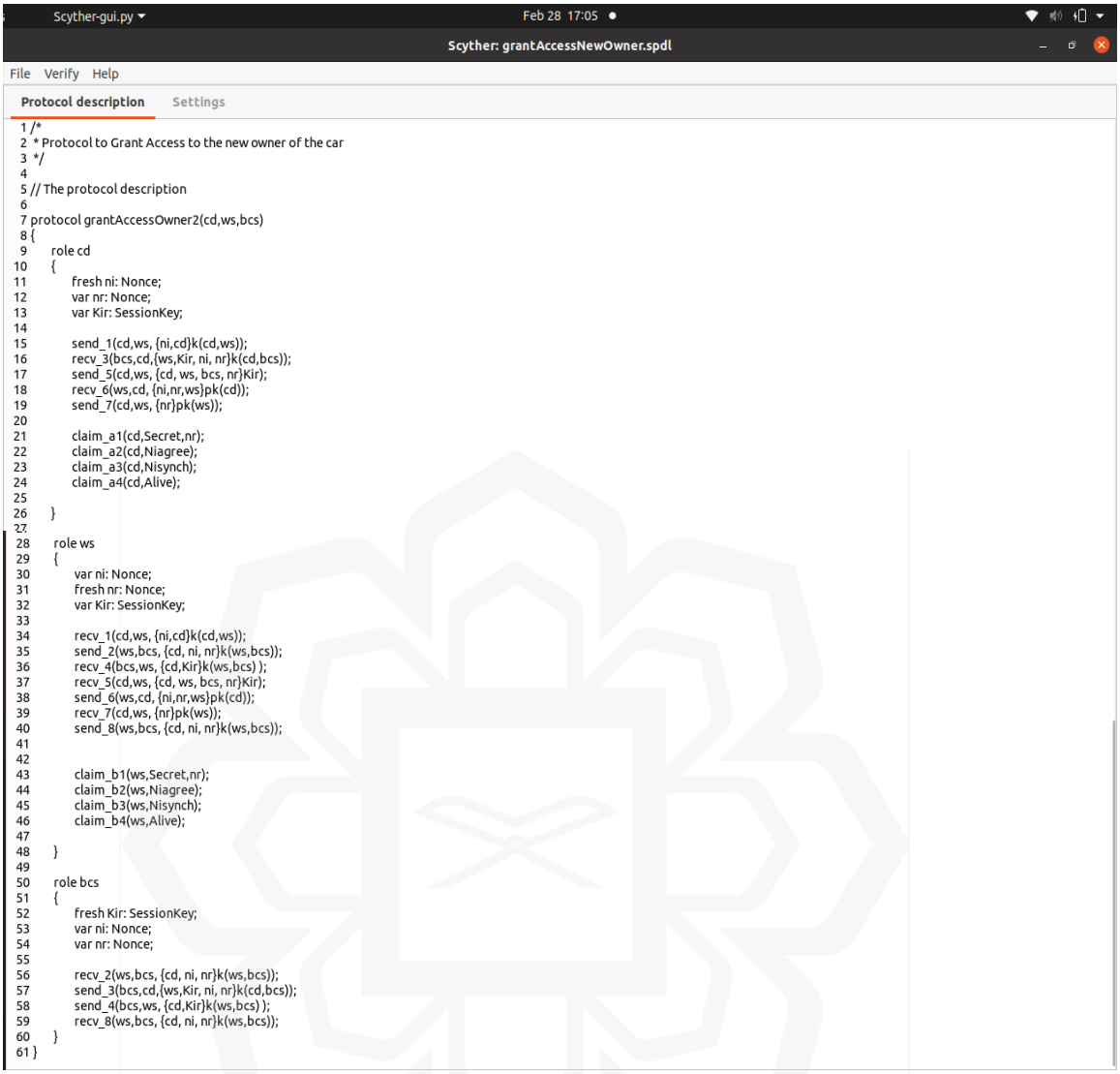


Figure 11 Scyther Code to Test the Security of Communication Protocol to Grant Access to the New Vehicle Owner

4.2.2.2 Testing Environment and Results

In the first round of testing, the protocol was examined using the Scyther Tool by following its default pre-set settings as shown in Figure 12 with a limit number of runs is five, which is fewer than the eight total communications that the protocol specifies. The outcome is

shown in Figure 13, which shows an overall status of 'Ok.'. However, the comments section shows that six out of eight claims are labelled as 'no attack within bounds.' Despite the overall 'Ok' status, these comments highlight potential vulnerabilities and indicate the presence of room for possible attacks within the protocol even with the overall status being "Ok."

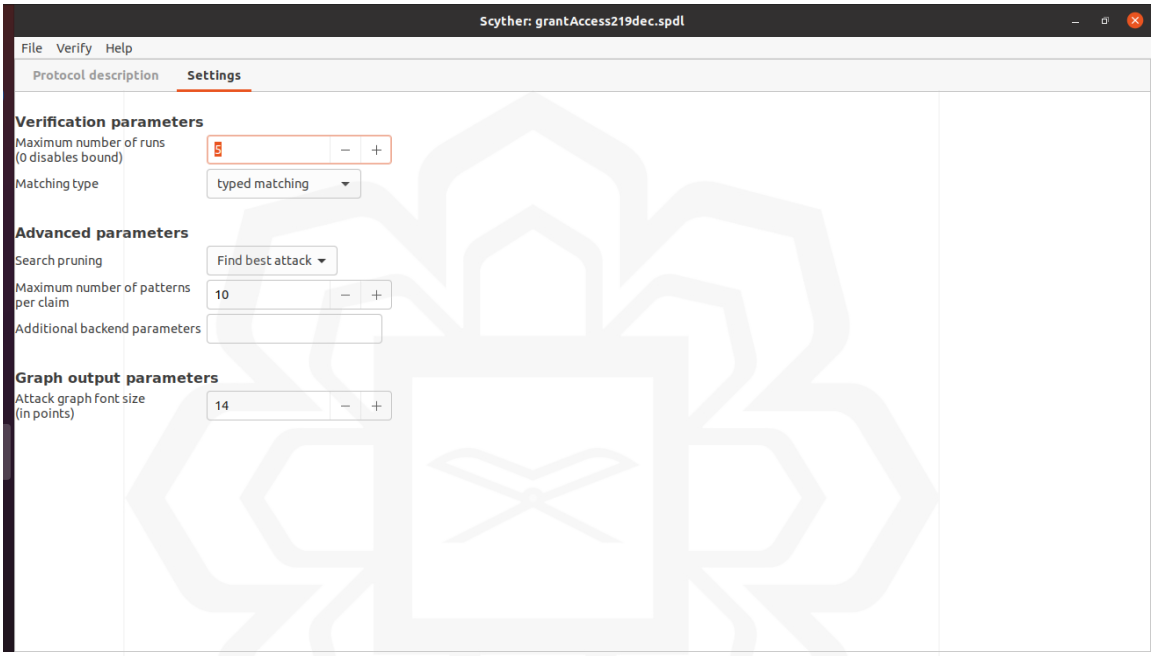


Figure 12 Pre-set Setting to Run Code in Scyther Tool

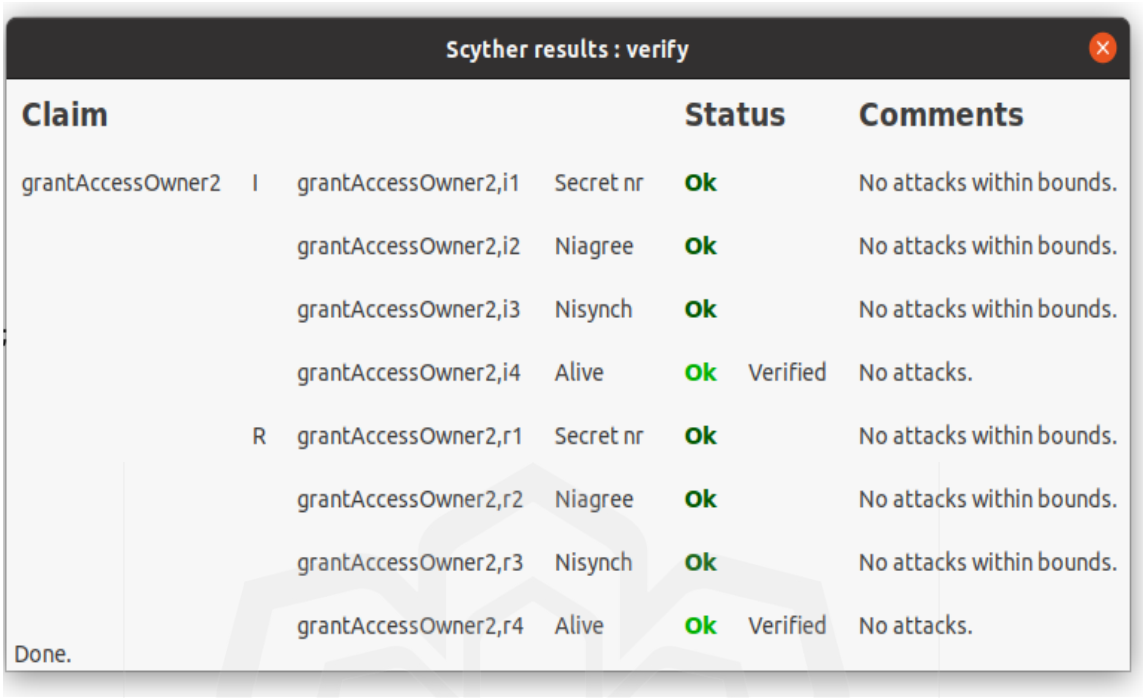


Figure 13 Result of Testing the Protocol using the Pre-set Setting of Scyther Tool

To eliminate the potential threats within the protocol, another test is carried out. This involves increasing the limit number of runs to ten, in which the value is higher than the total of eight communications specified in the protocol, as illustrated in Figure 14. The resulting analysis, captured in Figure 15, reflects an 'OK' and ‘Verified’ status. This designation signifies a comprehensive verification process showing that the protocol is immune to any threats and attacks.

The choice to extend the testing scenario beyond the initially specified number of communications gives an extra layer of assurance, ensuring that the protocol's resilience is tested comprehensively under varied conditions and scenarios. This robust testing methodology contributes to the protocol's overall reliability and effectiveness in safeguarding against potential vulnerabilities and security threats.

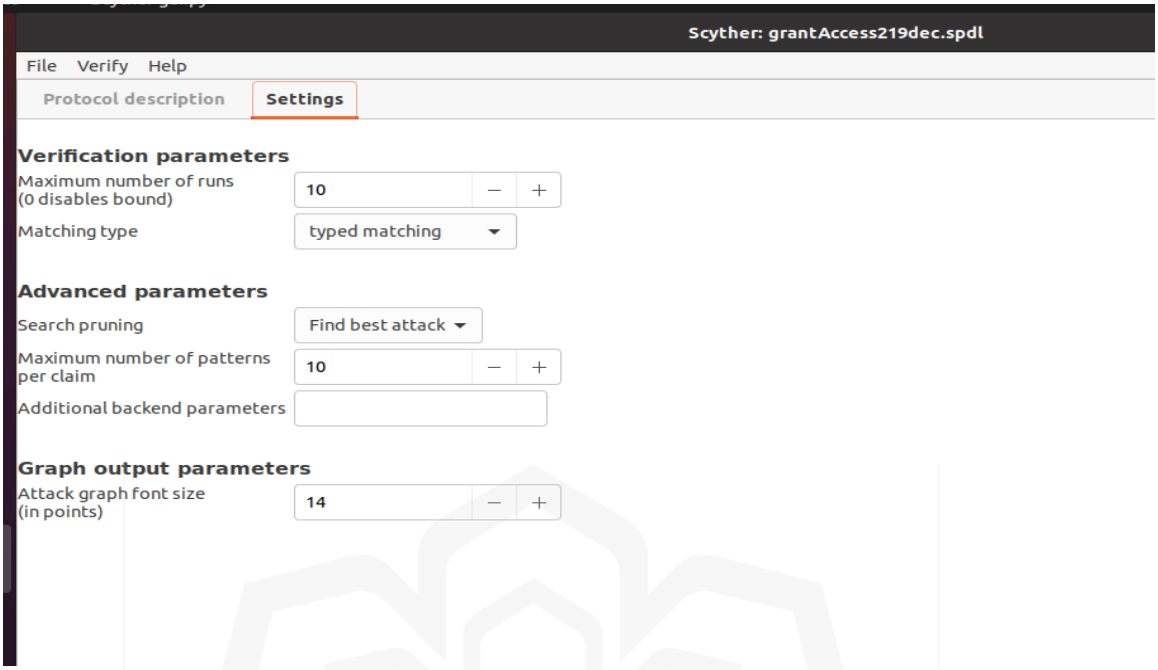


Figure 14 Customise Setting to Run Code in Scyther Tool

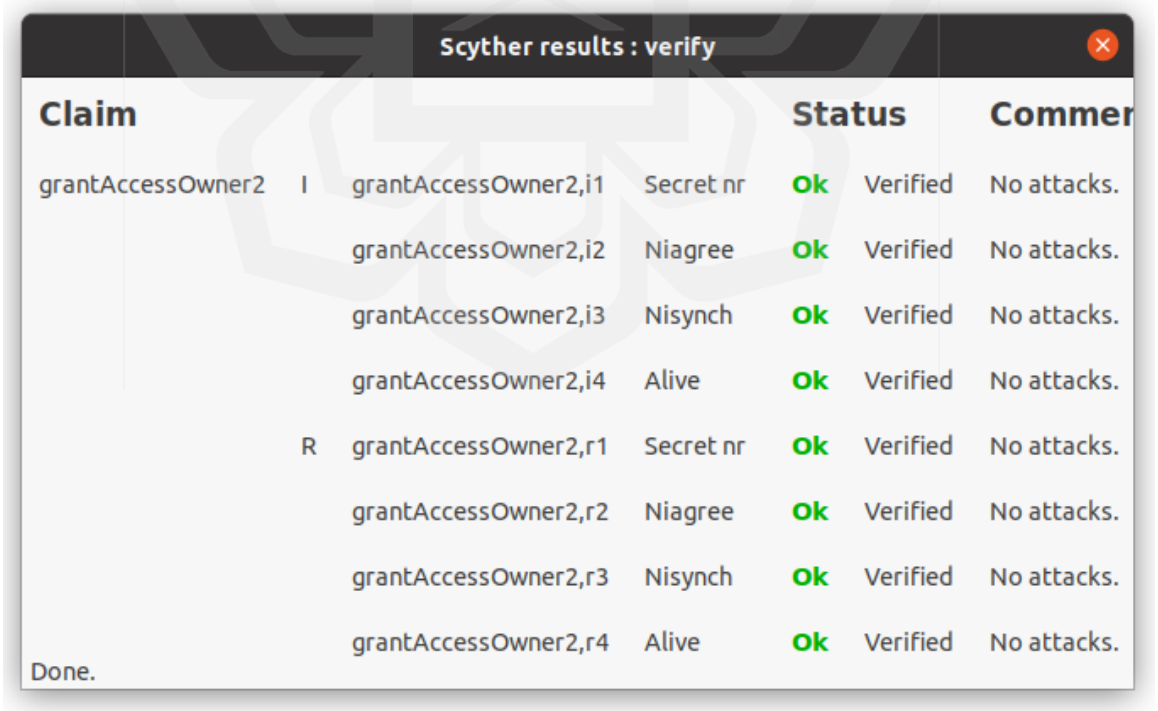


Figure 15 Result of Testing the Protocol using Customise Setting of Scyther Tool

4.2.2.3 Security Concerns and Testing Results

To incorporate the security properties that have been highlighted into the protocol specification within the testing script, the protocol has been tested using the claim events in Scyther Tool. This section provides an in-depth explanation of the security concerns and their respective claims that have been used in this research and the results after the claim events are tested in the Scyther Tool.

In the Scyther input scripts that have been run to test the communication protocol, the following security claims are made and verified.

1. Secrecy of the secret nonces (n_{cd} *and* n_{ws}).
2. Authentication properties, which include:
   a. Aliveness between CD and WS and aliveness between WS and BCS.
   b. Agreement between CD and WS of $n_{cd,}$ $n_{ws,}$ *and Kir*, agreement between WS and BCS of n_{cd} *and* n_{ws}, and agreement between WS and CD of n_{cd} *and* n_{ws}.
   c. Synchronisation between CD and WS and synchronisation between WS and BCS.

The first claim is secret which focuses on maintaining secrecy as a security property with a specific requirement for data confidentiality. In essence, this claim indicates that certain information must remain undisclosed to adversaries even when the communication is carried out over an unsafe network. The condition shows that when an agent engages with a non-compromised counterpart, the information shared should always be kept secret in any trace of the protocol. In the context of vehicle maintenance service records, secrecy guarantees that sensitive data such as ownership credentials and maintenance details will remain protected and only accessible by authorised stakeholders such as manufacturers, repair shops, and vehicle owners.

The second claim revolves around achieving agreement as a security property which is a requirement needed in providing data authentication. The fundamental idea behind the agreement is that all involved parties must reach a consensus on the values of variables. This is operationalised by ensuring that the contents of received messages align precisely with the sent messages, as specified by the protocol. In vehicle maintenance service records, the agreement helps to ensure that maintenance updates, diagnostic information and other critical data are accurately transmitted between stakeholders to preserve the integrity of records and foster trust among participants.

The third claim which is synchronisation, is the other way of achieving agreement as a security property, by adding a layer that requires both data and user authentication. This means that not only must the received messages correspond accurately to the sent messages as per protocol, but also verify that each received message has been sent by the designated communication partner. Synchronisation guarantees that updates to records occur in the proper order to ensure a consistent and reliable maintenance history that reflects the true sequence of service activities in the vehicle maintenance service records.

The fourth claim, which is aliveness, specifically focuses on users and data. In this context, the objective is to ensure that the communication is occurring in real-time, guaranteeing the authenticity of the participants involved in the communication. These tests also ensure that replayed or fabricated messages are invalidated to provide a foundation for accurate and secure protocol execution. In the context of vehicle maintenance service records, this guarantees that only authorised participants such as manufacturers, repair shops, and owners can contribute and be involved in the related communication process. Thus, the approach will help to safeguard the reliability of updates to maintenance data.

To conclude, all the claim events that are required in testing the communication protocol show the results of ‘OK’ which means the communication is verified safe from

any potential threats and attacks. The summary of the claim event, its properties and testing result is shown in Table 14.

Table 14 Summary of the Claim Events, its Properties and Testing Results

Security Properties (Claim Event)	Security requirements	Properties	Testing Results
Secrecy (Secret)	Data Confidentiality	Certain information must remain undisclosed to adversaries, even when communicated over an unsafe network. The condition stipulates that when an agent engages with a non-compromised counterpart, the information shared should always be kept secret in any trace of the protocol.	Secure from any attack
Agreement (Ni-Agree)	Data Authentication	The fundamental idea behind the agreement is that post-protocol execution, all involved parties must reach a consensus on the values of variables. This is operationalised by ensuring that the contents of received messages align precisely with the sent messages, as specified by the protocol.	Secure from any attack
Synchronisation (Ni-Synch)	User & data Authentication	Introduces an additional layer by requiring both data and user authentication. This means that not	Secure from any attack

		only must the received messages correspond accurately to the sent messages, as per the protocol, but also that each received message must be verified to have been sent by the designated communication partner.	
Aliveness (Alive)	User & Data Integrity	The objective is to ensure that the communication is occurring in real time, guaranteeing the authenticity of the participants involved in the communication process.	Secure from any attack

CHAPTER FIVE

DISCUSSION AND CONCLUSIONS

5.1 SUMMARY AND CONCLUSION

In the pursuit of enhancing the security of vehicle maintenance service records, this research has strategically formulated and addressed specific research questions. To enhance the security of these records, the study focused on identifying stakeholder responsibilities, establishing security requirements, and designing a secure framework complemented by a communication protocol. Each research question guided the systematic investigation into specific aspects of vehicle maintenance service records management.

This research presents the findings of a comprehensive list of stakeholders involved in the vehicle maintenance service records process. From that, their role is identified, and the security requirements have been addressed. Using the data gathered, two frameworks have been designed which are the framework for scheduled maintenance service and the framework for repair service. These frameworks implement consortium blockchain to ensure the transparency and integrity of maintenance records.

The development of a secure communication protocol which has been tested using the Scyther tool further solidified our findings. This testing process aimed to ensure the protocol is resilient against potential security threats to have secure vehicle maintenance service records. While this study primarily focuses on the grant access process for new vehicle owners, it lays the groundwork for future expansions to include data updates and maintenance verification.

This study makes contributions that go beyond technology. Our work fills a crucial need in the automobile sector by creating a safe and effective way to manage vehicle maintenance service records information. A crucial result is also the identification of stakeholders and their functions in the vehicle maintenance service records process. This data is essential for developing privacy regulations that are suited to the individual requirements of all parties involved and guarantee a thorough and inclusive approach to data security.

The designed frameworks not only facilitate real-time maintenance record keeping but also offer potential financial benefits. This is because proper maintenance service records management can help to prevent major breakdowns since it helps the owner to follow maintenance records timing and keep track of the records of their maintenance service as well as the vehicle part's lifetime. Additionally, the comprehensive maintenance history stored in the framework helps to add value to vehicles during resale which contributes to the economic life cycle of automobiles.

Our work expands the previous research by using knowledge from studies on automotive spare parts monitoring, cost prediction, sales management systems, and blockchain frameworks. Specifically, our contribution is noteworthy since it is a complete system designed to protect vehicle maintenance service records.

Table 15 summarises the research questions, key findings, and justifications, illustrating how each question was systematically addressed. This structured overview demonstrates the relationship between the research objectives, findings, and their relevance to overcoming challenges in vehicle maintenance service records.

Table 15 Summary of Research Questions, Findings, Results and Justification

Research Question (RQ)	Findings and Results	Justifications (How the RQ is Addressed)
RQ1: Who are the responsible stakeholders for the access, upload and maintenance of the vehicle maintenance service records?	Identified eight (8) stakeholders: manufacturers, dealers, vehicle owners, potential buyers, repair shops, technology teams, insurers and legislators.	The stakeholder list was validated through a literature review and checklist-based assessment, ensuring relevance to vehicle maintenance service records. Their roles were further analysed to define responsibilities, contributing to the accuracy, availability, and traceability of data in the system.
RQ2: What type of security requirements need to be included in handling the security of data?	Identified five (5) key security requirements: confidentiality, integrity, availability, data authentication, and user authentication.	Security requirements were derived using TVRA and STRIDE methodologies. These were mapped to threats like spoofing, tampering, and information disclosure, ensuring the system addresses all potential vulnerabilities while meeting industry standards for secure data handling.
RQ3: How to create a secure and trusted platform to store the history of vehicle	Designed two frameworks: one for scheduled maintenance services and one for	Frameworks address identified stakeholder interactions and security requirements. Consortium blockchain ensures

maintenance service records?	repair services, using consortium blockchain technology.	decentralisation, role-based access, and data immutability, improving record integrity and traceability. Validation through iterative feedback confirmed alignment with system objectives.
	Developed and tested a secure communication protocol for the grant access process using the Scyther Tool.	The protocol ensures secure data exchange during access provisioning by encrypting and authenticating data. Scyther Tool validated the protocol's resilience against threats like spoofing and tampering, ensuring reliability for digital forensics.

In conclusion, this research makes a pioneering contribution to the automotive industry by establishing a secure framework for the management of maintenance service records. The identified stakeholders, designed frameworks and secure communication protocols that have been tested, and future research directions collectively lay the groundwork for advancing the field and addressing the unique challenges in maintaining the security and privacy of automotive maintenance services.

5.2 FUTURE WORKS

Apart from all the contributions and significance of this study, there are still certain limitations that have been recognised. This research has primarily focused only on the local

car environment, and the designed protocol is specific to one phase only. Thus, the comprehensive solution would require additional protocols to cover other phases in the vehicle maintenance service records process.

Other than that, a comprehensive study of the designed framework needs to be done to have a thorough examination of the designed framework. It is an important step to ensure that every component and element of the framework is assessed and scrutinised. The validation process can identify in detail any potential weaknesses, inconsistencies, or areas for improvement within the framework can be identified and addressed.

A subsequent exploration focusing specifically on the vehicle data is essential to be carried out. The data is particularly focused on the information extracted from the Electronic Control Unit (ECU). The objective here is to identify crucial data points that are directly relevant to vehicle maintenance service records. This in-depth analysis is vital in uncovering essential information that can contribute significantly to the enhancement of security measures in handling such data. The outcomes of this investigation will serve as a valuable resource where additional insights into the security requirements necessary for the proper handling and protection of this data can be identified. Consequently, this further study is integral to refining and fortifying the security framework to ensure it aligns seamlessly with the vehicle data extracted from the ECU.

REFERENCES

Abbade, Lucas R., Ribeiro, Filipe M., Da Silva, Matheus H.M., & Álisson F.P., et al. (2020). Blockchain Applied to Vehicular Odometers. *IEEE Network*, (Vol. 34, No. 1, pp. 62-68).

Adam, M. (2022, August 16). 11 Best Automotive Scan Tools (for Home and Professional Use). https://cartreatments.com/best-automotive-scan-tools/

Bharati, M., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain-Based Cloud Computing: Architecture and Research Challenges. *IEEE Access (8)*, (pp. 205190-205205). https://doi.org/10.1109/ACCESS.2020.3036812

Brousmiche, K. L., Heno, T., Poulain, C., Dalmiere, A., & Hamida, E.B. (2018). Digitizing, Securing and Sharing Vehicles Life Cycle Over a Consortium Blockchain: Lessons Learned. *9th IFIP International Conference on New Technologies, Mobility and Security (NMTS).*

Butera, A., Gatteschi, V., Prattico, F., Novaro, D., & Vianello, D. (2023). Blockchain and NFTs-Based Trades of Second-Hand Vehicles. *IEEE Access, 11,* 57598-57615. https://doi.org/10.1109/ACCESS.2023.3284676

Chen, C.-L.; Zhu, Z.-P.; Zhou, M.; Tsaur, W.-J.; Wu, C.-M.; Sun, H. A Secure and Traceable Vehicles and Parts System Based on Blockchain and Smart Contract. *Sensors 2022*, *22*, 6754. https://doi.org/10.3390/s22186754

Dorri, A, Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, (pp. 119-125)

Elagin, V., Spirkina, A., Buinevich, M., & Vladyko, A. (2020). Technological Aspects of Blockchain Application for Vehicle-to-network. *Information, 11*(10), 465. https://doi.org/10.3390/info11100465

Fraga-Lamas, P., & Fernandez-Carames, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access*, *7,* 17578-17598

Franciosi, C., Di Pasquale, V., Iannone, R., & Miranda, S. (2021). Multi-stakeholder Perspectives on Indicators for Sustainable Maintenance Performance in Production Contexts: An Exploratory Study. Engineering, 27(2), 308-330. doi:10.1108/JQME-03-2019-0033

He X., Machanavajjhala A., Flynn C., & Srivasta D. (2017). Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage. *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communication*

Iftikhar, Z., Javed, Y., Abbas Zaidi, S. Y., Shah, M. A., Khan, Z. I., Mussadiq, S., &Abassi, K. (2021). Privacy preservation in resource-constrained IoT devices using blockchain—a survey. Electronics 10(1732), 1-26

Kathleen, E., Wegrzyn, & Eugenia Wang (2021, August 19). Types of Blockchain: Public, Private, or Something in Between. https://www.foley.com/en/insights/ publications/2021/08/types-of-blockchain-public-private-between/

Kei Leo, B., Thomas, H., Christian, P., Antoine, D., & Elyes Ben, H. (2018). Digitizing, Securing and Sharing Vehicles Life-cycle Over a Consortium Blockchain: Lessons Learned. *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* (pp. 1-). https://doi.org/10.1109/NTMS.2018.8328733

Kevin Klaus, G. B., Christopher, C., & Hans-Joachim, H. (2021). A generalized approach to automotive forensics. *Forensics Science International: Digital Investigation,* (Vol.36)

Kieseberg, P., Malle, B., Frühwir, P., Weippl, E., & Holzinger, A. (2016). A Tamper-Proof Audit and Control System for The Doctor in The Loop. *Brain Informatics*, 1-11

Laborda, J., & Moral, M. J. (2020). Automotive Aftermarket Forecast in a Changing World: The Stakeholders' Perceptions Boost! Sustainability, 12, 7817. https://doi.org/10.3390/su12187817

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Supplementary Material - Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst*, *24(1),* 131–143

Lin, C.Y., Chang, M.C., Chiu, H.C., & Shyu, K.H. (2016). Secure Logging Framework Integrating with Cloud Database. *International Carnahan Conference on Security Technology*

Lin, W.-Y., Lin, F. Y.-S., Wu, T.-H., & Tai, K.-Y. (2020). An On-Board Equipment and Blockchain-Based Automobile Insurance and Maintenance Platform. Advances on Broad-Band Wireless Computing, Communication and Applications (Proceedings of the 15th International Conference on Broad-Band and Wireless Computing, Communication and Applications (BWCCA-2020)) (Vol. 159, pp. 223-232).

Meyliana, Surjandy, Fernando, E., Eka Widjaja, H. A., Cassandra, C., Tan, A., Carolina, M., & Carolina, M. (2021). Blockchain Technology for Vehicle Maintenance Registration. *2021 International Conference on Information Management and Technology (ICIMTech), Jakarta, Indonesia* (pp. 608-613). doi: 10.1109/ICIMTech53080.2021.9534974

Mohamad-Ali, N., Raja Ghazilla, R. A., Abdul-Rashid, S. H., Sakundarini, N., Ahmad-Yazid, A., & Stephenie, L. (2018). End-of-Life Vehicle Recovery Factors: Malaysian Stakeholders' Views and Future Research Needs. Sustainable Development, 2018, 1–13. https://doi.org/10.1002/sd.1741

Moon, J., Kim, D., Kim, J., & Jeon, J. (2021). The Migration of Engine ECU Software from Single-Core to Multi-Core. *IEEE Access, 9,* 55742-55753.

Najdenova, I. (2019). Blockchain-Based Approach for Preserving Car Maintenance History (Master Project). Swiss Federal Institute of Technology Lausanne. Retrieved from [/https://www.epfl.ch/labs/dedis/wp-content/uploads/2020/01/report-2018_2-iva-najdenova-car.pdf]

Pandit, A., & Gupta, S. (2021, February). Tackling substitution fraud in remanufactured product warranty service. *International Journal of Latest Engineering Research and Applications, 6(2)*, 09-18. https://www.researchgate.net/publication/351103408

Preikschat, K., Böhmecke-Schwafert, M., Buchwald, J., & Stickel, C. (2021). Trusted Systems of Records Based on Blockchain Technology - A Prototype for Mileage Storing in the Automotive Industry Concurrency Computed Pract Exper. 2021. https://doi.org/10.1002/cpe.5630

Rahul, K., Ateet, P., Shyam, K. S., & Kadam, R. S. (2022). Car & Motor Vehicles Sales and Maintenance. *IRE Journals*, (Vol. 6, Issue 1, pp. 183-186)

Ray, I., Belyaev, K., Strizhov, M., Mulamba, D., & Rajaram, M. (2013). Secure Logging as a Service: Delegating Log Management to the Cloud. *Syst. Journal IEEE, 7,* 323-334.

Sharma, P., Kumar, N., & Park, J. (2019). Blockchain-Based Distributed Framework for Automotive Industry in a Smart City. *IEEE Transactions on Industrial Informatics*, (Vol. 15, No. 7, pp. 4197-4205)

Xu, R., Hang, L., Jin, W., & Kim, D. (2021). Distributed secure edge computing architecture based on blockchain for real-time data integrity in IoT environments. *Actuators, 10(8),* 197. https://doi.org/10.3390/act10080197

Yeh, K., Su, C., & Cha, S. (2023). Special Issue Editorial "Blockchain-Enabled Technology for IoT Security, Privacy and Trust". *Symmetry, 15(5),* 1509. https://doi.org/10.3390/sym15051059

Zhonghui, S., Yanying, G., Zhonghong, S., Shouchen, Y., & Baoyu, H. (2023). Maintenance cost prediction for the vehicle based on maintenance data. *Proceedings of the Institution of Mechanical Engineers*, Part D: Journal of Automobile Engineering. https://doi.org10.1177/09544070221147080

LIST OF PUBLICATIONS

Che Saufi, N. N., **Mohd. Ab Razak, N. S.**, & Mansor, H. (2019). FoRent: Vehicle Forensics for Car Rental System. *Proceedings of the 3rd International Conference on Cryptography. Security and Privacy (ICCSP'19)*. Presented at Kuala Lumpur, Malaysia: Association for Computing Machinery (pp. 153-157). https://doi.org/10.1145/3309074.3309101

Mohd. Ab Razak, N. S., Mansor, H., Sharmin, S. (2023). A Secure Framework for Vehicle Maintenance Service. *2023 12th International Conference on Software and Computer Applications (ICSCA 2023)*. Presented at Kuantan, Malaysia. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3587828.3587861