Sticky-PRE: A Sticky Proxy Re-Encryption Protocol for Persistent Vehicle Data Privacy

Ashish Ashutosh[1], Omar Hasan[2], Pratik Baishnav[3], Harald Kosch[4], Lionel Brunie[5]

***Abstract*— Connected vehicles generate a vast amount of data and share it with external entities such as the cloud, neighboring vehicles, Road-Side Units (RSUs), and other third-party services in a Vehicle to Everything (V2X) setting. This data is vulnerable and can lead to the leakage of personal information of vehicle owners, such as driving habits, travel routes, and identity theft, among others. Moreover, with the implementation of the General Data Protection Regulation (GDPR), it becomes imperative to empower users with control over their data and the ability to choose whom they share it with. To address this objective, we present a protocol that utilizes a combination of sticky policies and a proxy re-encryption scheme. This protocol ensures that user-defined access controls on the data persist even when crossing organizational boundaries and addresses the confidentiality, integrity, and accountability of vehicle data. Furthermore, we assess our protocol using a semi-honest threat model and analyze its vulnerabilities. Lastly, we perform a quantitative analysis of the data flow model to observe the system's performance.**

I. INTRODUCTION

Modern vehicles connect and communicate with other vehicles, infrastructures, and networks via wireless technologies such as dedicated short-range communication or a cellular data connection. This has resulted in a large volume of data being generated and shared in a connected vehicle ecosystem. For example, measuring physical parameters, location, and driving behaviour, often several times per second, can generate an estimate of 25 GB of data per hour [1]. Vehicle manufacturers' intentions to upload 50–70% of such data carry significant implications for policymakers, manufacturers, and local network infrastructure [2].

Consequently, cybersecurity attacks have risen over time, causing concerns among data owners regarding the security and privacy of their vehicle data [3]. Highlighting the vulnerabilities in a modern vehicle, a group of researchers from Keen Security Lab were able to gain remote access to the infotainment and telematics unit of several BMW models via the wireless interfaces [4]. In a survey on attacks on connected vehicles, authors highlighted that with the increase in 4G and 5G communication technologies, wireless attacks have become a major threat, and measures are required to address them [3]. In another study to observe the state of data privacy in vehicles, four vehicles were evaluated for privacy and concluded that none of them were compliant with the European General Data Protection Regulation (GDPR) because it was possible to access personal and vehicle data [5].

Some works in the literature have tried to address the privacy concerns. As an illustration, in a survey focusing on privacy in automotive applications, cryptographic techniques like Public Key Infrastructures (PKIs) and digital signatures were identified as mechanisms to protect specific attributes of vehicle location and vehicle ID [6]. In another work, a digital twin-based privacy enhancement model was proposed that identified privacy risks and anomalies using machine learning on sensor data and performed anonymization to minimize privacy risks [7]. In a blockchain-based solution for privacy, the data is stored in-vehicle, and only upon verification of the data consumer can the vehicle owner reveal the data using a key [8].

While existing approaches use cryptographic techniques, anonymization, and blockchain to strengthen privacy, they do not enforce the data owner's consent and decisions across the data life-cycle. In a survey, 15 drivers who were aware of their data being processed were interviewed and preferred that their choices were upheld throughout the data life-cycle [9] In the connected vehicle ecosystem, data is continuously generated, transmitted, and stored across stakeholders such as vehicles, cloud platforms, and service providers. Thus, the data is beyond the original data owner's direct control.

This introduces complex and connected vehicle-specific data-sharing challenges, such as location-based restrictions, time constraints, and limits on the frequency of data shared with third parties. Unlike static access control, the connected vehicle environment requires dynamic, context-aware, and enforceable mechanisms that persist with the data, especially when it is shared with untrusted or semi-trusted third parties. Therefore, there is a need for a policy enforcement paradigm that not only controls data access but also travels with the data and can be securely enforced in different contexts.

To address this gap, this paper explores the following research question: *RQ*: How can vehicle data be shared while enforcing the data owner's consent and ensuring data confidentiality, particularly during third-party transfers? To enforce the data owner's consent throughout the data life-cycle, especially in cases with third-party transfers, we propose a novel protocol using a sticky policy approach. Sticky policy is a mechanism where machine-readable policies are

[1]Ashish Ashutosh is with the Faculty of Computer Science and Mathematics, University of Passau, Germany. ashish.ashutosh@uni-passau.de

[2]Omar Hasan is with the Department of Computer Science, INSA Lyon, France. omar.hasan@insa-lyon.fr

[3]Pratik Baishnav is with the Faculty of Computer Science and Mathematics, University of Passau, Germany, baishn01@ads.uni-passau.de

[4]Harald Kosch is with the Faculty of Computer Science and Mathematics, University of Passau, Germany. harald.kosch@uni-passau.de

[5]Lionel Brunie is with the Department of Computer Science, INSA Lyon, France. lionel.brunie@insa-lyon.fr

coupled to the data, and the coupled policies travel with the data throughout its life-cycle [10][11][12]. Furthermore, to address the confidentiality of vehicle data and enhance the sticky policy enforcement, we use a proxy re-encryption (PRE) scheme in our protocol. We chose PRE because, in a study by Tang [13], the PRE scheme was found to perform best with sticky policies.

The remainder of the paper is structured as follows: Section II presents a scenario that realizes the privacy-related challenges in connected vehicles. Section III presents the state of the art. Section IV introduces PRE and its properties. Section V proposes the Sticky-PRE protocol. In Section VI, we evaluate the model based on semi-honest adversaries. Section VII presents the performance of the protocol. Finally, we conclude our findings in Section VIII.

II. Vehicle Data Sharing Scenario

In this section, we present a scenario that highlights the privacy-related challenges that a user may face in a connected vehicle ecosystem in the real world.

Consider *Alice*, a resident of *Passau, Germany,* who recently purchased a new car. She owns her vehicle data. She enrolled with a motor insurance company named *Smart-Surance*. *SmartSurance* is a data-centric company that aims to provide better service based on collected user data. *SmartSurance* gathers information on her driving habits to tailor her insurance policy and provide her with discounts on her monthly premiums. This type of insurance is commonly known as usage-based motor insurance [14]. It plays a crucial role in promoting traffic safety, reducing pollution emissions, and easing traffic congestion [14].

To monitor Alice's driving characteristics and identify the risk indicators to calculate the monthly premium, *Smart-Surance* requires access to a set of attributes - *speed, time, and location (latitude and longitude)* [14], [15]. Data are recorded on a vehicle telematics device, and the medium to collect data depends on the telematics manufacturer but generally involves the use of the On-Board Diagnostics (OBD) II port [15]. Alice is willing to share the attributes required by *Smartsurance* because she wants to avail herself of tailored premiums that reflect her specific circumstances, potentially providing her with monetary benefits. Additionally, she wants to use value-added services to avoid traffic congestion.

While *Alice*, the vehicle owner, is open to sharing data, she chooses to impose specific restrictions on what *SmartSurance* can collect.

- Alice wants to keep her travels outside Passau confidential to prevent location-based profiling. Consequently, she chooses *not* to disclose her *location* data (latitude and longitude) when departing from *Passau*
- During *weekends* (Saturday and Sunday) and on *weekdays between 8 PM and 8 AM*, she prefers *not* to share her location and speed data.
- Alice has expressed her willingness to share her location data; however, she has requested to *limit* it to *one data point per minute* to avoid being tracked too closely.

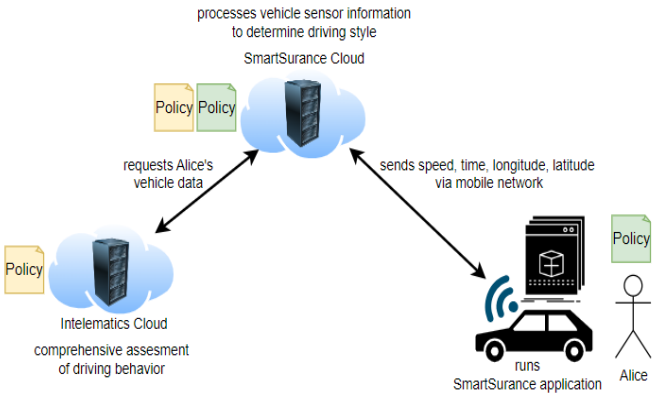

Fig. 1. Data Sharing Scenario in a Connected Vehicle Ecosystem

To use SmartSurance, Alice must also share her vehicle data attributes - *speed and location (latitude and longitude)* to a third-party telematics company named *Intelematics*, which serves as the *Data Controller*. Intelematics evaluates driving behaviour and risk, providing SmartSurance with precise and thorough assessments. The machine-readable policies specify the restrictions imposed by Alice and the conditions for the usage of her data by the data controllers. Note that there are two different types of policies in place, as highlighted in *green* for the privacy policy and in *yellow* for the data processing policy in Figure 1. A policy agreement between a data owner and a data controller, i.e., *Alice* and *SmartSurance* is a *privacy policy* that specifies the restrictions imposed by Alice. A policy agreement between the two data controllers, i.e., *SmartSurance* and *Intelematics* is a *data processing policy* that specifies the conditions under which the data should be processed. Both data controllers are required to adhere to the privacy and data processing agreement as outlined in the policies to ensure compliance with the GDPR.

Alice, SmartSurance, and Intelematics encounter various privacy-related challenges. For instance, when Alice shares her vehicle data with SmartSurance, she becomes concerned about data security and the risk of unauthorized access or breaches, potentially leading to identity theft or other privacy breaches. Alice is also apprehensive about the potential misuse of her data and whether it might be shared with third parties without her consent. Consequently, SmartSurance must adhere to regulations governing the storage and utilization of Alice's vehicle data, including safeguarding it against cyberthreats by implementing robust security measures. For example, unauthorized access to Alice's location data could compromise her privacy by revealing details about her workplace or residence. Failure by SmartSurance or Intelematics to comply with these regulations could result in up to 4% of their total global turnover of the preceding fiscal year under GDPR [16].

III. State of the Art

The outlined use case highlights the need for a robust access control mechanism that ensures data confidentiality

and integrity and respects user-defined policies in a dynamic and decentralized automotive ecosystem. While traditional access control models offer varying degrees of security and flexibility, they often struggle to enforce fine-grained, persistent policies when data moves across different entities.

To address these challenges, sticky policies have emerged as a mechanism that binds access control policies directly to the data, ensuring that policies remain enforceable regardless of where the data resides [17][10][11]. This approach is particularly useful in a connected vehicle ecosystem, where vehicle-generated data may be accessed by multiple third-party service providers under different conditions.

Miorandi et al. conducted a recent state-of-the-art survey of sticky policies, but no work was found where the sticky policy approach was used in a connected vehicle context [12]. This could be because connected vehicles require complex policies where environmental parameters such as location, time, and frequency of access need to be considered. Sticky policies accompany the data, and if they navigate across organizational boundaries, encryption of the data becomes necessary. Subsequently, we look into protecting the data when such policies accompany it.

Recent advancements in vehicle data protection during sharing have introduced de-identification techniques such as homomorphic encryption, suppression, pseudonymization, k-anonymity, differential privacy, and federated learning [18]. While these approaches enhance privacy, they often involve significant computational demands and communication overhead, necessitating further research. Furthermore, blockchain technology has been proposed to provide decentralization, immutability, and transparency in data-sharing frameworks. However, challenges related to scalability, resource constraints, and data privacy persist, limiting its widespread adoption in vehicular networks [8].

In an analysis by Tang [13] of different encryption schemes such as Public-Key Encryption (PKE), Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), and Proxy Re-Encryption (PRE) with sticky policies, PRE performed the best. Additionally, PRE was found to have mitigated the key management issue on behalf of the data owner [13]. This is important in a real-world scenario because an average person would not have the know-how to handle cryptographic keys regularly. In the work proposed by Tang, the data owner is also responsible for generating the re-encryption keys. This would not fit in the context of connected vehicles because it would require the availability of the data owner for generating the keys, which violates the decoupling between data owners and data consumers proposed in our work.

While sticky policies enforce data handling procedures, they do not inherently provide data confidentiality. Thus, encryption mechanisms such as PRE are necessary to ensure Alice's data remains protected while being shared.

IV. Building Block: Proxy Re-Encryption

We use Proxy Re-Encryption (PRE), a cryptographic mechanism that permits secure delegation of decryption rights while maintaining data secrecy, to address the issues with regulated and secure data sharing that have been noted in the state-of-the-art. PRE has an entity called a proxy that transforms a ciphertext from one public key to another without learning anything about the underlying data [19]. Nuñez et al. performed a thorough analysis of different PRE schemes and their application in secure access delegation and found that 80% of their bibliometric analysis, in which *confidentiality* was the objective, PRE was used [19]. In this paper, we refer to their work to analyze PRE construction and identify the key properties applicable to our vehicle data sharing scenario [19].

The main properties associated with most PRE schemes are *directionality, number of uses, collusion-safeness, transitivity, interactivity, temporary, conditional, non-transferability, proxy invisibility, and perfect key-switching* [19]. For our data-sharing scenario, the following properties are relevant:

1) Unidirectional: A proxy re-encryption scheme is considered unidirectional if the data producer can delegate the decryption rights to the data consumer and not the other way around [19]. In contrast, in a bidirectional scheme, it is possible for the data consumer to delegate decryption rights to the data producer. In our vehicle data-sharing scenario, the trust relationship between *Alice* and *SmartSurance* is not symmetric, and thus we focus on a unidirectional PRE scheme where Alice delegates the decryption rights to SmartSurance. An important difference between the two is that with the bidirectional scheme, the secret keys of the data producer and the data consumer are needed to generate the re-encryption key, whereas only the secret key of the data producer is needed in unidirectional schemes.
2) Limited Multi-Use (Structure): A limited multi-use PRE scheme allows ciphertexts to be re-encrypted multiple times (depending on the multi-hop parameter). This is used in PRE schemes with a single ciphertext space. In contrast, in a single-use PRE scheme, the ciphertexts can be re-encrypted only once. It is linked to PRE schemes with multiple cyphertext spaces because re-encryption can be made as one-way transformations between cyphertext spaces [19]. In our date-sharing scenario, we use a multi-use structure because it performs better with encryption, decryption, and re-encryption operations [19].
3) Collusion-safeness: This characteristic indicates the safeness of the data producer's secret key against collusion attacks initiated by both the data consumer and the proxy [19]. In our scenario, it means that Alice's secret key sk_A cannot be derived from the re-encryption key $rk_{A\rightarrow B}$ and SmartSurance's secret key sk_S. This is important because, in case the proxy is colluding with SmartSurance, the proxy cannot recover the private key of Alice. Otherwise, a malicious proxy could decrypt the data of Alice.
4) Non-interactive: The proxy re-encryption scheme is

said to be non-interactive if the secret key of the data consumer is not required in the generation of the re-encryption key. That is to say, the re-encryption key is generated using the data producer's key pairs and the data consumer's public key. In our scenario, the re-encryption key for re-encrypting Alice's data is generated as: ReKeyGen(pk_A,sk_A,pk_S) $\rightarrow$ $rk_{A\rightarrow S}$. We need a non-interactive scheme because it reduces communication overhead and protects against collusion attacks for deriving the secret keys involved [19].

We looked through various PRE schemes that had these properties [20][21][22][23] but faced two key challenges: (a.) the codebase was not available to experiment with; (b.) they did not support defining complex policies that considered environmental factors in a connected vehicle ecosystem. To address these challenges, we sought open-source repositories that offer PRE schemes and a framework for defining complex policies.

OpenFHE is an open-source library that provides proxy re-encryption for BGV, BFV, and CKKS schemes in C++ [24][25]. Additionally, it is also maintained regularly, with the last stable release being October 2024 [26]. Furthermore, to create complex policies in a connected vehicle ecosystem that allowed defining location, time, and frequency in their policy definition, we use the XACML4M framework because it was defined to handle policies specifically for the connected vehicle ecosystem [27]. Based on this analysis, our approach integrates OpenFHE's PRE capabilities with XACML4M's policy framework to achieve privacy-preserving vehicle data sharing with fine-grained policy enforcement.

V. Sticky-PRE Protocol

In this section, we propose our *Sticky-PRE* protocol to address vehicle data sharing while enforcing the data owner's decisions throughout the data life-cycle and providing data confidentiality with third-party transfer protection. The main idea is to couple the policy and the data together to enforce the data owner's decisions. Furthermore, to ensure data security, we employ a two-step encryption process. First, the data is encrypted within the vehicle using Alice's public key. Then, a proxy re-encrypts the data before securely transferring it to a third party. Before delving into the details of this protocol, we present the objectives of the protocol, the entities involved and the assumptions made in our system.

A. Objectives

The objectives of our protocol concerning privacy are specified below.

- Objective 1 (O1) - Data Confidentiality: Ensure that vehicle data remains confidential and protected from unauthorized access or disclosure throughout its lifecycle, i.e., during transmission, storage, and processing.
- Objective 2 (O2) - Data Integrity: Guarantee the integrity and trustworthiness of vehicle data by preventing unauthorized modification and ensuring that data remains accurate.
- Objective 3 (O3) - Access Control: Implement robust access control mechanisms to regulate access to vehicle data based on predefined policies, ensuring that only authorized entities can access data in accordance with the policy.
- Objective 4 (O4) - Policy Enforcement: Sticky policies accompany data and dictate its handling based on predefined constraints. The system ensures policy compliance before granting access. The system also protects policy integrity by hashing policies (SHA-128) and verifying their integrity before execution.
- Objective 5 (O5) - Data Accountability: Establish mechanisms such as logging for enforcing compliance with data-sharing policies for transparency purposes.

B. Entities

- Data Producer: Alice's vehicle - It generates vehicle data that's encrypted with Alice's public key before being sent outside the vehicle, often to the cloud for storage.
- Data Consumers: SmartSurance and Intelematics - A data-centric insurance and telematics organizations, respectively, that aim to provide better service based on collected user data.
- Storage: The encrypted data that leaves the vehicle is coupled with a hash of the relevant policy. This data is then stored in a database typically managed by the vehicle manufacturer.
- Trusted Authority (TA): An entity that the data owner trusts and has delegated the responsibility for key management and protection of their vehicle data. It generates the Public Key (P_k) and Secret Key (S_k) for data owners (Alice), data consumers (SmartSurance and Intelematics) and the Re-Encryption Key ($rk_{a->b}$) for a given pair of public/secret Keys for the proxy. It consists of two independent sub-components of eXtensible Access Control Markup Language (XACML):
  1) Policy Enforcement Point (PEP): receives all incoming requests from the data consumer for access to the data producers' data.
  2) Policy Decisions Point (PDP): receives the request from the PEP and evaluates it based on stored policies. After processing the request, it makes a decision to *permit/deny* access and forwards the decision to the PEP for the decision enforcement.
- Proxy: receives the re-encryption keys from the TA and re-encrypts the data based on the decision made by the PDP. It uses a *re-encryption key database* to fetch the re-encryption key to be applied based on the identity of the requesting entity.

C. Sticky-PRE Protocol

The Sticky-PRE protocol consists of five key phases: sticky encryption, incoming request, request processing, re-encryption, and response phase (see Figure 2). They are detailed below.

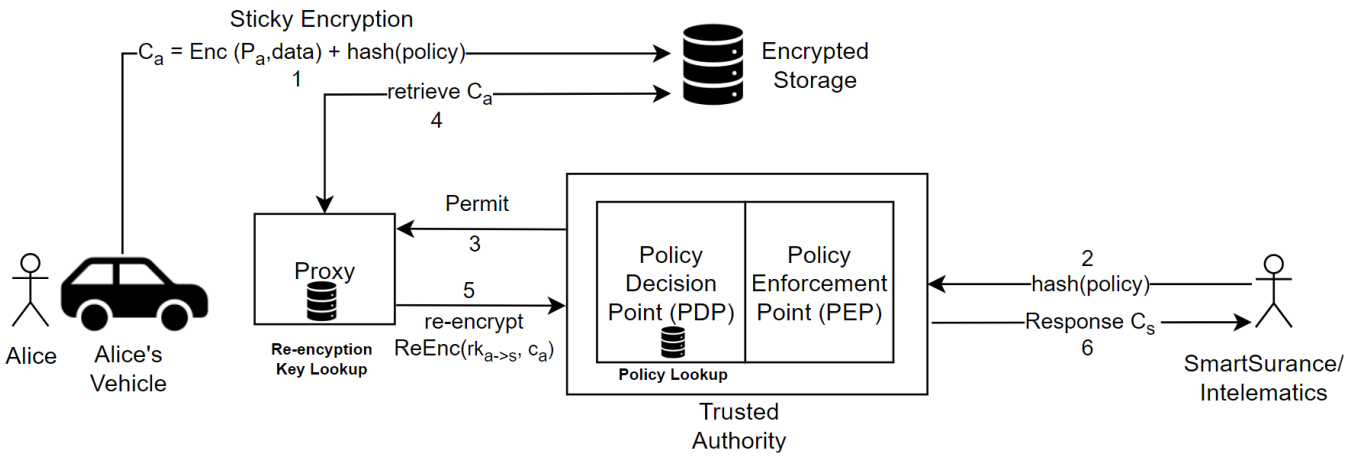

Fig. 2. Sticky-PRE Protocol for Connected Vehicles. The phases are: (1) Sticky Encryption, (2) Incoming Request, (3) Request Processing, (4) Re-Encryption and (5) Response.

1) Sticky Encryption: The data owner's vehicle performs two key operations before the data is sent out of the vehicle for storage.
   a) Data Encryption: The data is encrypted using the data owner's public key Pk_A.
   b) Stick Policy Hash: A hash of the policy is coupled with the encrypted data.
2) Incoming Request: The data consumer requests access to the data by sending a hash of the policy to the trusted authority.
3) Request Processing: The trusted authority evaluates the request as described below:
   a) Policy Enforcement Point (PEP): The PEP receives the incoming request from the data consumer and transforms it into an XACML request and forwards it to the PDP. If the decision received from the PDP is a *permit*, then it forwards it to the *Proxy*; otherwise, it responds to the data consumer with *access denied*.
   b) Policy Decision Point (PDP): The PDP performs a *policy lookup* in its policy database and evaluates the XACML request by fetching the required attributes and makes a decision to *permit/deny*. Then, it forwards its decision to the PEP.
4) Re-Encryption: The proxy, upon receiving a *permit*, performs two operations:
   a) It retrieves the corresponding cyphertext and re-encryption key of the data owner from the *Encrypted Storage* and *re-encryption key lookup* database, respectively.
   b) Then, it re-encrypts the cyphertext using the re-encryption key and sends it to the PEP.
5) Response: The PEP then returns the re-encrypted cyphertext to the data consumer, which can then be decrypted only using the data consumer's secret key Sk_B.

Algorithm 1 gives a brief overview of the Sticky-PRE protocol between Alice and SmartSurance. Our implementation of the proposed Sticky-PRE protocol can be accessed at [28].

Algorithm 1: Secure Vehicle Data Sharing with PRE and Sticky Policies

Input: Vehicle Data (VD), Policy (P), Alice's Public Key (Pk_A), SmartSurance Public Key (Pk_S)
Output: Encrypted Data (EVD) accessible by SmartSurance

// Setup
VDD Server stores (P, hash(P)) in H2 database
Generate ((Pk_A), (Sk_A), $rk_{A\to S}$ using OpenPRE

// Data Encryption by Alice's Vehicle
EVD $\leftarrow$ Encrypt(VD, Pk_A)
Store (EVD, hash(P)) in H2 database

// SmartSurance Requests Access
SmartSurance $\rightarrow$ VDD: (credentials, hash(P))
VDD matches hash(P) with stored policies
If no match $\rightarrow$ Reject Request

// Policy Decision Evaluation
VDD $\rightarrow$ PDP: (Request Attributes)
PDP evaluates P using XACML4M
If decision = PERMIT $\rightarrow$ Continue
Else $\rightarrow$ Reject Request

// Re-Encryption Process
VDD $\rightarrow$ PRE Server: (EVD, SmartSurance Credentials)
PRE Server authenticates SmartSurance
REVD $\leftarrow$ ReEncrypt(EVD, $rk_{A\to S}$)
Store REVD in directory

// Data Delivery
VDD $\rightarrow$ SmartSurance: (REVD)
SmartSurance decrypts REVD using Sk_S

VI. Threat Evaluation

In this section, we perform an informal threat evaluation of our proposed Sticky-PRE protocol. The protocol that we consider here is in the presence of *Static Semi-Honest* or

also known as *Honest but Curious adversaries* [29]. The adversary adheres strictly to the protocol, yet it may attempt to gain unauthorized insights by examining the transcript of received messages and its internal state [29]. This represents a weak adversary model, but a secure data flow model under semi-honest adversaries guarantees the prevention of *inadvertent leakage* of information [29]. It proves beneficial when parties primarily trust each other but aim to prevent any record of their input elsewhere [29].

We begin by identifying the sensitive attributes and stakeholders in our vehicle data-sharing scenario. Subsequently, we analyze the threats posed by an adversary in our proposed Sticky-PRE protocol. We evaluate whether our objectives defined in Section V-A were satisfied by our protocol. In the end, we give an overview of the security of our proposed protocol.

Before we proceed, we would like to state our assumptions: (1.) we assume that the *TA* is fully trusted to simplify the privacy guarantees provided by our protocol. The TA will act in the best interest of the system and the data owner, ensuring the confidentiality and integrity of the data. (2.) We assume that the *proxy* is partially trusted because it may attempt to gather unauthorized insights by examining the transacted messages.

A. Analysis of Sensitive Information

In a survey on privacy regulations and privacy-related attacks, it was found that privacy-related attacks can be categorized into *location inferencing, driver fingerprinting, and driving behavior analysis* [30]. They computed a Privacy Score (PS) to quantify the privacy risk linked to data from a particular vehicular sensor. It was found that the top three riskiest sensors were *location, current speed, and steering wheel angle* [30]. In our vehicle data sharing scenario presented in Section II, the attributes collected by *SmartSurance* are *speed, time, and location*. Thus, based on the above analysis, we will consider *location and speed* as sensitive information in our data flow model. Note that for the sake of simplicity, we only consider single sensitive attributes and not quasi-identifiers. For example, quasi-identifiers such as location and time of travel can be combined to reveal patterns of when and what routes are taken by Alice to work.

B. Privacy Preserving Measures

Table I presents different privacy threats. Additionally, it also gives the privacy-preserving measures taken in the Sticky-PRE protocol to address these threats while satisfying the objectives defined in Section V-A. Note that a threat can address multiple objectives.

Summarizing the security of the Sticky-PRE protocol below:

- Data Confidentiality: The protocol ensures data confidentiality by encrypting the vehicle data using the data owner's public key before it leaves the vehicle for storage. This ensures that only authorized entities with the corresponding private key can decrypt and access the data.
- Data Integrity: By attaching a hash of the policy with the data, access to data is granted only after the policy conditions have been satisfied. Thus, protecting any modification to the data. Furthermore, hashing the policy offers two benefits: (1.) ensuring the integrity of the policy, and (2.) reducing the size of lengthy policies, which can be advantageous for minimizing data packet sizes during network transmission and speeding up the policy retrieval for evaluation.
- Access Control: The protocol employs access control mechanisms through policy enforcement points (PEP) and policy decision points (PDP) to regulate access to the data. Access requests are evaluated based on stored policies, and access is granted or denied accordingly. Furthermore, it supports evaluating complex policies such as location, time and frequency-based access to vehicle data, which is necessary in the connected vehicle context.
- Distributed Access: The protocol involves multiple entities, including the data producer (vehicle), trusted authority (TA), data consumers, and proxy. In addition, there could be multiple instances of the TA and proxy. This distributed architecture allows for access to the data from multiple locations and ensures resilience against single points of failure.
- Data Accountability: The trusted authority (TA) is responsible for granting access after the policy constraints have been evaluated and obligations met. Furthermore, the data is encrypted using a cryptographic mechanism and strongly associated with the policies [31]. Thus, providing transparent and traceable handling of data. Furthermore, logging is enabled in case of audit requirements.

Therefore, we have addressed our research question on how vehicle data can be shared while enforcing the data owner's decisions and addressing data confidentiality and third-party transfer protection.

VII. Quantitative Evaluation

We complement the threat evaluation with an experimental evaluation where we measure the following performance metrics:

- Encryption Time: The time it takes to encrypt the data using the public key of Alice Pk_A.
- Re-Encryption Time: The time it takes to re-encrypt the data using the re-encryption key $rk_{A \to S}$ by Proxy.
- Decryption Time: The time it takes SmartSurance to decrypt the data using the secret key of the third party Sk_S.
- Policy Evaluation Time: The time it takes for XACML4M to evaluate the policy.

Our execution environment was an AMD Ryzen 5 @ 3.60 GHz processor with 12GB of RAM. Table II gives an overview of the main operations performed during the execution of the sticky-PRE protocol. These figures were measured over 10,000 executions for each operation. To

TABLE I

THREAT ANALYSIS FOR THE STICKY-PRE PROTOCOL

Threat	**Sticky-PRE Protocol**
O1, O2: A malicious entity sniffs network traffic for information	Sensitive attributes *location and speed* are encrypted with Alice's public key (Pk_A) inside the vehicle before the data is exposed to the network. Furthermore, when the *proxy* fetches the cyphertext, it only has access to the re-encryption keys ($Rk_{A->S/I}$) and is only able to re-encrypt the cyphertext without being able to access the original data. Additionally, PRE schemes are resistant to chosen plaintext attacks and chosen cyphertext attacks. Thus, guaranteeing data confidentiality over the network.
O1, O2, O3: If SmartSurance is malicious and tries to access unauthorized data	Every access request is made by sending a hash(policy) to the TA. A sub-component of TA, i.e., the PDP evaluates the request based on the policy and the access permissions. If SmartSurance were to request unauthorized data access, then the hash(policy) will not match and access will be denied by the TA.
O1, O2: If the proxy is malicious and tries to gain insight into the data during re-encryption	The responsibility of the Proxy is to re-encrypt the data with the re-encrpytion key ($Rk_{a->b}$) provided by the TA. Note that a proxy re-encryption scheme which is unidirectional, collusion-safe, and non-interactive cannot access or modify the original data while re-encrypting. The data can only be accessed by the secret key (Sk_A) of Alice before re-encryption or the secret key of SmartSurance/Intelematics ($Sk_{S/I}$) after re-encryption. The proxy does not have access to either of the secret keys. Thus, the protocol provides data confidentiality and data integrity.
O1, O2, O3: If the proxy and SmartSurance were to collude together and attempt to access unauthorized data	When the TA evaluates the incoming request from SmartSurance then it would deny access if the request was invalid. Additionally, the PRE scheme used is uni-directional and non-interactive, meaning that PRE does not have any means to access Alice's private key to perform decryption on the original data.
O1, O2: If a malicious user gains access to the storage	The storage unit receives encrypted data from the vehicle, and it stays encrypted inside the database. It can be decrypted only with Alice's secret key (Sk_A) to which neither the vehicle manufacturer nor the malicious entity has access. Therefore, the data is protected.
O2, O4: Policy tampering—an attacker may attempt to modify or forge policies to gain unauthorized access	Policies are hashed using SHA-128 and stored securely in the H2 database. If any modification is detected, the request is automatically denied.

contextualize our results, we compare them with the findings from Deng et al.[32] and [19]. In [32], the IBE scheme reported encryption and decryption times of 46.9 ms and 43.78 ms, respectively. In comparison, our Sticky-PRE protocol using the PRE (Brakerski/Fan-Vercauteren (BFV)) scheme achieves approximately 4.7× faster encryption and 5.5× faster decryption performance.

In comparison to the implemented PRE schemes discussed in [19], our proposed Sticky-PRE protocol demonstrates competitive performance. Specifically, our PRE scheme outperforms AFGH06a (Encr: 22.76 ms, Re-Encr: 83.52 ms, and Decr: 13.76 ms), LV11a (Encr: 155.27 ms, Re-Encr: 386.93 ms, and Decr: 443.87 ms), and WDLC10a (Encr: 22.52 ms, Re-Encr: 22.29 ms, and Decr: 11.89 ms) by a significant margin. It also marginally performs better than BBS98 PRE scheme (Encr: 11.07 ms, Re-Encr: 11.48 ms, and Decr: 11.21 ms). In contrast, the ABPW13 and NAL15a PRE schemes performed better because they were high-performance lattice-based schemes.

Nonetheless, a direct comparative analysis remains challenging due to differences in experimental setups, such as hardware, libraries used, and programming languages. Furthermore, our protocol uniquely integrates fine-grained policy evaluation (0.02 ms), which is not addressed in [32][19], highlighting the practicality of our approach in real-world access control scenarios for connected vehicles.

TABLE II

PERFORMANCE OF DIFFERENT OPERATIONS IN A STICKY-PRE PROTOCOL

	Encryption	**Re-Encr**	**Decryption**	**PolicyEval**
PRE scheme	10ms	10ms	8ms	0.02ms
CPU Load	2.58%	2.4%	3.82%	NA
Memory (JVM)	71MB	82MB	87MB	94MB

VIII. CONCLUSION

In a connected vehicle ecosystem, data is vulnerable and has led to privacy concerns for the data owners. In this paper, we illustrated an example use case highlighting the challenge of upholding the owner's consent in a data-sharing scenario with third parties. To address this, we proposed the Sticky-PRE protocol, which combines machine-readable policies that remain attached to the data throughout its life-cycle with a proxy re-encryption (PRE) scheme that enables secure and conditional access in a connected vehicle setting.

Key features of our Sticky-PRE protocol include fine-grained access control using XACML4M, support for access delegation, data confidentiality, integrity, accountability, and persistent vehicle data privacy. We presented a simple threat analysis based on an honest-but-curious model, followed by a quantitative performance evaluation. By combining policy enforcement with cryptographic techniques, the Sticky-PRe protocol provides a practical solution to the research question of sharing vehicle data while enforcing the data owner's consent. As our next step, we intend to conduct a threat analysis based on a fully adversarial model and formalize it.

REFERENCES

[1] F. Richter, "Big data on wheels [digital image]," 2017. https://www.statista.com/chart/8018/connected-car-data-generation/.

[2] C. Dickert, "Network overload? adding up the data produced by connected carse," 2023. https://www.visualcapitalist.com/network-overload/.

[3] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, "Attacks and defences on intelligent connected vehicles: a survey," *Digital Communications and Networks*, vol. 6, no. 4, pp. 399–421, 2020.

[4] "Researchers hack bmw cars, discover 14 vulnerabilities," 2018. https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.

[5] M. Cheah, S. Haynes, and P. Wooderson, "Smart vehicles: The data privacy smog," in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 82–87, 2018.

[6] V. H. Le, J. den Hartog, and N. Zannone, "Security and privacy for innovative automotive applications: A survey," *Computer Communications*, vol. 132, pp. 17–41, 2018.

[7] V. Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry," in *2018 International Conference on Intelligent Systems (IS)*, pp. 272–279, 2018.

[8] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[9] A. Dowthwaite, D. Cook, and A. L. Cox, "Privacy preferences in automotive data collection," *Transportation Research Interdisciplinary Perspectives*, vol. 24, p. 101022, 2024.

[10] G. Karjoth, M. Schunter, and M. Waidner, "Platform for enterprise privacy practices: Privacy-enabled management of customer data," in *Privacy Enhancing Technologies* (R. Dingledine and P. Syverson, eds.), (Berlin, Heidelberg), pp. 69–84, Springer Berlin Heidelberg, 2003.

[11] M. Mont, S. Pearson, and P. Bramhall, "Towards accountable management of identity and privacy: sticky policies and enforceable tracing services," in *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, pp. 377–382, 2003.

[12] D. Miorandi, A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Sticky policies: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 12, pp. 2481–2499, 2020.

[13] Q. Tang, "On using encryption techniques to enhance sticky policies enforcement," *DIES, Faculty of EEMCS, University of Twente, The Netherlands*, 2008.

[14] D. I. Tselentis, G. Yannis, and E. I. Vlahogianni, "Innovative motor insurance schemes: A review of current practices and emerging challenges," *Accident Analysis Prevention*, vol. 98, pp. 139–148, 2017.

[15] S. Husnjak, D. Peraković, I. Forenbacher, and M. Mumdziev, "Telematics system in usage based motor insurance," *Procedia Engineering*, vol. 100, pp. 816–825, 2015. 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2014.

[16] "General data protection regulation gdpr," 2018. https://gdpr-info.eu/.

[17] G. Karjoth, M. Schunter, and M. Waidner, "Privacy-enabled services for enterprises," in *Proceedings. 13th International Workshop on Database and Expert Systems Applications*, pp. 483–487, 2002.

[18] S. Löbner, F. Tronnier, S. Pape, and K. Rannenberg, "Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing," in *Proceedings of the 5th ACM Computer Science in Cars Symposium*, CSCS '21, (New York, NY, USA), Association for Computing Machinery, 2021.

[19] D. Nuñez, I. Agudo, and J. Lopez, "Proxy re-encryption: Analysis of constructions and its application to secure access delegation," *Journal of Network and Computer Applications*, vol. 87, pp. 193–209, 2017.

[20] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," vol. 9, p. 1–30, feb 2006.

[21] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in *Topics in Cryptology–CT-RSA 2009: The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*, pp. 279–294, Springer, 2009.

[22] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1786–1802, 2011.

[23] Y. Polyakov, K. Rohloff, G. Sahu, and V. Vaikuntanathan, "Fast proxy re-encryption for publish/subscribe systems," *ACM Transactions on Privacy and Security (TOPS)*, vol. 20, no. 4, pp. 1–31, 2017.

[24] A. A. Badawi, J. Bates, F. Bergamaschi, D. B. Cousins, S. Erabelli, N. Genise, S. Halevi, H. Hunt, A. Kim, Y. Lee, Z. Liu, D. Micciancio, I. Quah, Y. Polyakov, S. R.V., K. Rohloff, J. Saylor, D. Suponitsky, M. Triplett, V. Vaikuntanathan, and V. Zucca, "Openfhe: Open-source fully homomorphic encryption library." Cryptology ePrint Archive, Paper 2022/915, 2022. https://eprint.iacr.org/2022/915.

[25] OpenFHE, "Welcome to openfhe's documentation," 2024. https://openfhe-development.readthedocs.io/en/latest/.

[26] . Contributers, "Openfhe - open-source fully homomorphic encryption library," 2024. https://github.com/openfheorg/openfhe-development.

[27] A. Ashutosh, A. Gerl, S. Wagner, L. Brunie, and H. Kosch, "Xacml for mobility (xacml4m)mdash;an access control framework for connected vehicles," *Sensors*, vol. 23, no. 4, 2023.

[28] S.-P. Protocol, 2024. https://github.com/PtkVs/Sticky-PRE–A-Sticky-Proxy-Re-Encryption-Protocol-for-Persistent–Vehicle-Data-Privacy.git.

[29] Y. Lindell, *How to Simulate It – A Tutorial on the Simulation Proof Technique*, pp. 277–346. Cham: Springer International Publishing, 2017.

[30] M. D. Pesé and K. G. Shin, "Survey of automotive privacy regulations and privacy-related attacks," 2019.

[31] S. Pearson and M. Casassa-Mont, "Sticky policies: An approach for managing privacy across multiple parties," *Computer*, vol. 44, no. 9, pp. 60–68, 2011.

[32] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," *Information Sciences*, vol. 511, pp. 94–113, 2020.