A user privacy-centric access control policy of data for intelligent transportation systems

Rémi Adelin, Eric Alata, Vincent Migliore, Vincent Nicomette

A user privacy-centric access control policy of data for intelligent transportation systems

Rémi Adelin, Éric Alata, Vincent Migliore, Vincent Nicomette
LAAS-CNRS, Université de Toulouse, CNRS, INSA, Toulouse, France
{remi.adelin, eric.alata, vincent.migliore, vincent.nicomette}@laas.fr

***Abstract*—Intelligent Transportation Systems have a variety of application, from improving transportation safety and traffic management to infotainment. The development of these systems includes the deployment in the vehicle of sensors that collect data and share them with actors having different profiles, roles and motivations. These data may concern the private life of drivers, who, most of the time, are not aware of the recipients and of the usage of their data. A key issue is to give to drivers control of their data. For that purpose, we propose in this paper a flexible and fine-grained access control policy of data, based on Attribute-Based Encryption, designed to protect drivers privacy. We also provide a description of the security architecture to enforce such an access control.**

***Index Terms*—fined-grained access control, attribute-based encryption, kp-abe, intelligent transportation systems**

I. Introduction

Vehicles are today inseparable from our daily activities. They are equipped with a multitude of sensors, actuators and calculators that improve users driving comfort through multiple services. Some services go beyond drivers needs and may interest several actors. For example, drivers geolocation, used for real-time navigation, is also useful to have a more detailed view of the global traffic and may help other drivers to better position themselves in the traffic. A motion sensor may be useful for maintenance services to analyse the state of the roadway and be aware of the sections that must be refurbished urgently. The connectivity addition in vehicles allows services development for diverse stakeholders (such as manufacturers, equipment suppliers, service providers) and drivers are no longer the only recipients of the result of data processing from sensors of their own vehicle. Therefore, these data need to be stored and accessible by these different actors in order to be processed. Storage is today mainly performed in the Cloud.

Data collected in vehicles are thus a major concern, especially for the different actors that are supposed to benefit from these data processing. On one hand, for data that are usually processed to provide additional services, drivers should have the choice to send them to providers if they consider that they must be private. On the other hand, exceptional situations may require that data considered private must be transmitted to a sworn organisation (in case of an accident for example). Today, the European legislation, through the GDPR [1], is in favour of drivers, but technical solutions still have to be implemented to enforce this directive. Such enforcement is crucial today because attacks targeting privacy of end users have been regularly increasing during the latest years (especially in the Cloud or social network environment [2]), and there is no doubt that they will soon target private information from connected vehicles.

To take into account the duality privacy/legality, the technical solution should consider three issues. First, data stored in the Cloud must not be accessible by the Cloud provider in plaintext. Second, the driver can adapt the access rights to a specific actor or a group of actors. Third, in case of exceptional situation management, a specific actor (i.e., *sworn* organisation) can override these restrictions, temporarily.

In this context, encryption is an essential trail. Usual approach based on so-called Public Key Infrastructure (PKI) is mainly designed to secure point-to-point communications. As Intelligent Transportation Systems are fundamentally multi-providers (a data can be used by several third parties), directly transposing PKI in this scenario leads to turn all broadcasting operations into point-to-point ones, inducing a complex and costly management of communications and certificates. A first element of answer to this problem is group encryption. A group scheme associates to a public key a set of private keys. However, this scheme does not easily take into account data sending to multiple groups and requires either to encrypt data for each group, either a new group creation leading to key generation and distribution.

A more robust solution in this context is the use of Attribute-Based Encryption (ABE). ABE is similar to group encryption, but with the decisive advantage that it only requires one encryption key for a large combination of possible groups. It is based on the combination of attributes (that act as keys) and access trees (that act as locks). Keys are provided along with the ciphertext, and if the recipient have the right lock, then it can decrypt the message (more details are provided in the dedicated section). This property makes sense in the context of connected cars, because access rights to actors may vary depending on time and location of the actor itself (typically for licensing purpose) or the vehicle (typically for privacy purpose). In this article, we provide a dynamic, fine-grained, privacy-centric access control policy of collected data based on ABE. In an ideal world, privacy should be determined only by users. However, today, in the face of the web giants, the balance of power is against users who do not have the ability to protect themselves. In our opinion, to balance this relationship, it is essential that users have the support of a trusted authority.

The rest of the paper is organised as follows: Section II provides a brief overview of ABE. A state of the art of ABE in the context of vehicular networks is presented in Section III. Section IV depicts the access control policy while Section V describes the architecture overview enabling to enforce this policy. Section VI draws conclusions.

II. Attribute-Based Encryption

ABE is an asymmetric encryption scheme enabling access control over encrypted data. ABE is split into two constructions: Cipher-

Policy Attribute-Based Encryption (CP-ABE) [3] and Key-Policy Attribute-Based Encryption (KP-ABE) [4]. Both constructions are based on the combination of attributes and access trees. Access trees are composed of leaves and nodes, where leaves are attributes and nodes are logical operators. A ciphertext can be decrypted only if attributes satisfy the access tree. For CP-ABE, the access tree is included into the ciphertext while attributes are included into secret decryption keys. In KP-ABE, the access tree is included into secret decryption keys while attributes are included into the ciphertext. A **Trusted Authority**[1] (TA), with a so-called master key, is responsible for assigning, in the case of CP-ABE, attributes into the decryption keys, and in the case of KP-ABE, an access tree into the decryption keys.

In our case KP-ABE seems a more suitable construction than CP-ABE. The benefits of using KP-ABE over CP-ABE is the fact that encryption is much more natural and simple. Attributes can be seen as tags that modify which group has access to the data. In previous CP-ABE scenario, access control policy is a complex access tree that combine different kind of attributes. In our scenario, privacy can be reduced to a single attribute that indicate a certain type of data should be considered private. Moreover, a high quantity of data will be emitted by vehicles in the context of vehicular communication and the bandwidth is a key resource which impacts the selection of the encryption scheme. KP-ABE is preferable than CP-ABE from this point of view, because in CP-ABE the ciphertext size is greater since information related to the access tree has to be sent.

Let's illustrate the KP-ABE scheme with the following example. A user *U* works for a company *C* in a town *T*. During working hours, he takes his own vehicle for business trips. During such trips, he wants to share his geolocation with *C* but not outside working hours to preserve his privacy. If *U* is victim of an accident, a sworn organisation must be able to decrypt data only if they were issued in T_vicinity. The access tree is specified using attributes representing the data type (*gps*), contextual information (geographical: *T*, *T_vincinity* and temporal: *day*), the role of the actor (*C*) and a privacy criticality level (*low*). C negotiates with the TA the following access tree contained in its secret key: $gps \wedge C \wedge day \wedge T \wedge low$. The sworn organisation needs to decrypt data in T_vincinity, its associated access tree contains restriction which are only temporal or geographical: $T\_vincinity$. During working hours, gps data are encrypted with the following attributes: *gps*, *C*, *day*, *T*, *T_vincinity* and *low*. Outside working hours, the attributes used are: *gps* and *T_vincinity*.

A KP-ABE scheme consists of four algorithms: Setup, KeyGen, Encrypt and Decrypt.

Setup(λ): This algorithm is executed by the TA to generate the system keys. It takes as input a security parameter λ. It outputs the public key **PK** and the master key **MK**.

KeyGen(MK, A): This algorithm is executed by the TA to generate a key for a user. It takes as input the master key **MK** and an access tree **A**. It outputs a secret key **SK**.

[1]This authority is a trusted non-profit organisation. We assume that this authority is not compromised. To protect against attacks, this authority uses security mechanisms like intrusion detection. These security mechanisms are outside the scope of this article.

Encrypt(PK, M, S): This algorithm is executed by a user to share data using attributes. It takes as input the public key **PK**, a message to encrypt **M** and a set of attributes **S**. It outputs a ciphertext **CT** containing the attributes and the ciphermessage.

Decrypt(CT, SK): This algorithm is executed by a user to decrypt a ciphertext. It takes as input a ciphertext **CT** and a secret key **SK**. It decrypts the ciphertext if the set of attributes **S** defined in the ciphertext **CT** verifies the access tree **A** contained in the secret key **SK** and outputs the message **M**.

Our objective is to enforce a privacy preserving access control policy in the context of connected vehicles. ABE is a good candidate because it enables, with a limited set of security keys, to manage a dynamic evolution of authorised users, while allowing issuers to have a real control of the scope of data they encrypt. In addition, unlike usual access control solutions requiring prior authorisation of access to data, ABE eliminates this step reducing the number of exchanges required at protocols level.

III. Related works

The use of ABE in the context of connected cars has been studied initially for vehicle-to-vehicle communications (V2V) and extended to vehicle-to-Cloud communications (V2C) in Vehicular Adhoc NETwork (VANET). In 2008, Hong et al. [5] provides the first blueprint of the use of ABE in VANETs without any performance analysis. In 2009, this paper is extended with performance analysis, but at this point no anonymity, authentication, misbehavior detection nor revocation are achieved. After that, a vast majority of papers focus on optimisation and securisation of message dissemination in VANETs, but not directly on privacy. In [11] a solution is proposed to reduce the number of key updates after the departure of a group member. In [7], authors address the problem of policy enforcement in a situation with compromised Road Side Unit (RSU) and provide a security and performance analysis of their solution. In [8], the authors focus on message dissemination using an ancestor of ABE. They proposed an application of their solution intended to information dissemination for emergency management. In [12], the authors reduce the computation time in VANET via a constant number of operations during decryption. In [9], a message dissemination scheme is proposed with decryption computation outsourced on RSU. More recently, a message dissemination scheme using ABE for access control and a Cloud as data storage has been described in [10].

Most applications proposed in those papers are essentially focused on efficient message dissemination. The control of driver's privacy is not clearly stated as those papers do not focus on privacy.

Other authors focus on access control of data issued by service providers [13], [14]. They propose to use ABE to grant access to services data according to the licence of subscribers. In those work, the privacy of data sent from vehicle to those services is not address.

Our position is to propose a framework to enable such privacy control.

IV. Privacy preserving access control policy

A. System overview

The system we consider is composed of vehicles, a Cloud platform, different actors, and a trusted authority. Each vehicle stores to the Cloud information from its sensors and actuators. Depending

on licences provided, different actors can request information to the Cloud. To manage access rights, the trusted authority is responsible of the licensing which guarantee both security and privacy.

1) Actors considered: The **manufacturer** produces and sells or leases the vehicle to the driver, but also benefits from vehicles data to better manage his car fleet. He is also likely to take advantage of these data by proposing them to various organisations.

Equipment suppliers are in charge of the design of one or more systems embedded in the vehicle. They can collect data through their systems to study how well their systems work.

Given the amount of data to store, a data warehouse in the Cloud is essential. A **Cloud provider** is therefore also an actor to consider. Its role should be limited to store or even process data but it should not consult data without drivers knowledge.

Business partners are actors intended to make profits from data exploitation. For example, a meteorology service may be interested in data from temperature sensors of vehicles while a market research firm may be interested in different geolocation surveys to identify an ideal commercial location. A driver must have the possibility to accept that a certain category of business partners have access to some of his data while denying access to others.

An **insurance company**, in case of an accident, may be interested in accessing data sent during the accident. However, drivers must have the possibility to deny permanent access to data because the company could use these data to adjust their contract. The company must therefore have access to data only in case of accidents, and only during a specific time window.

Finally, the **driver**'s journey and habits reveal many aspects of his behaviour. For example, the speed of his vehicle can be used to identify possible infraction and his stops can reveal his favourite places. It is important to preserve his control over his personal data as much as possible.

2) Adversary considered: Our framework mainly targets curious adversaries. The objective of such adversary is to extract information that current privileges do not grant access to. Our framework is able to prevent the following attacks.

Man-in-the-middle: the adversary cannot decrypt communications from vehicle to Cloud, from Cloud to actors and from trusted authority to actors.

Curious Cloud employee: the adversary has no access to any information stored in the Cloud, including any cryptographic keys.

Collusion between several actors: the adversary cannot increase its privileges by combining its privileges with another actor's privileges.

Attacks that are not addressed by our framework are considered in the scope of the jurisdiction (actor that broadcast information legally obtained, compromised vehicles that send plain data, ...). The framework is also considered as a work base that can evolve in order to address additional attacks.

B. ABE attributes and access tree design

1) Attributes: In the context of connected vehicles, we propose four kind of attributes: data type related (such as motor, board, temperature, ...), contextual information (geographical and/or temporal), role related (such as manufacturer, equipment supplier, ...) and privacy related. These attributes are not intended to be exhaustive, we suggest them for illustrative purposes. The datatype, role and contextual attributes are not related to privacy. They are always included and cannot be customised by drivers. The only attributes that are customised are privacy attributes. Such kind of attributes are included by following an access control policy that is defined by drivers. During encryption, the cryptographic module included in the car determines which level of criticality is associated to this specific data and select the right attributes. We consider that three levels of criticality are necessary for flexibility, but for compact solutions, a unique attribute is feasible.

An interface in the vehicle would enable drivers to specify for each data the privacy attributes. As a vehicle may have multiple drivers, the set of attributes selected for data encryption is realised with respect to drivers. This selection is realised at vehicle start, the driver must authenticate himself before starting to drive.

If we transpose this solution to CP-ABE, the access control policy should have been coded into the access tree (which is defined at encryption time in CP-ABE). Consequently, the access tree would have been complex, which is not desirable in CP-ABE because complexity is correlated to the access tree complexity. Our solution has the main advantage that the access control policy is no longer coded inside the ABE cryptosystem, but just deported as software pre-processing to select the right privacy-related attributes.

2) Access trees: The access trees are defined per actor jointly with the TA. They are expressed as a set of disjunctions and conjunctions relative to attributes. They must at least take into account public information about the actor, licencing information and privacy information. Public information are related to the actor's role, in order to restrict access to specific type of data. Licencing information provides the flexibility to limit the access depending on time and location (licence valid for 3 years, only in a specific countries, during week-ends only,...). Privacy information further limit the access to data. This privacy information is the only one that can be bypassed by construction, for example to allow legal authorities to decrypt the message when an accident occurs. The bypass implementation is straightforward, it is sufficient to construct a specific access tree that does not use privacy attributes.

Depending on the fineness of the policy, the associated access tree can be quite complex. However, this complexity has a limited impact in KP-ABE since the access tree is integrated into the decryption key, which is sent only once.

V. Security Architecture

Figure 1 presents the proposed security architecture based on the four algorithms that describe KP-ABE. During **system setup** ①, the TA executes the Setup algorithm and generates the public key PK and the master key MK. During **manufacturing** ②, the public key PK is deployed inside vehicles, together with mandatory attributes. Note that both the PK and mandatory attributes can be updated during system operation. When actors wants to **subscribe** ③ to the system, they request for a new secret key associated to a desired access tree. The TA is in charge of verifying the match between the access tree and the actor role. Then, the TA executes the KeyGen algorithm to generate the actor's secret key containing the requested access tree and sends through a secure channel this secret key to the actor. When drivers enter their vehicle, they have to provide the access control policy that must be followed by the cryptographic module. While driving, generated data are encrypted according to

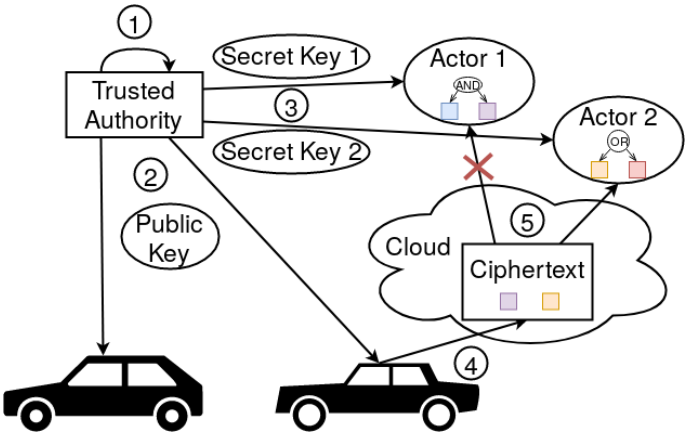

Fig. 1. Architecture

privacy attributes and mandatory attributes. Then, encrypted data are **sent** to the Cloud ④. Only actors with a compatible access tree can **decrypt** and read data ⑤ with the Decrypt algorithm.

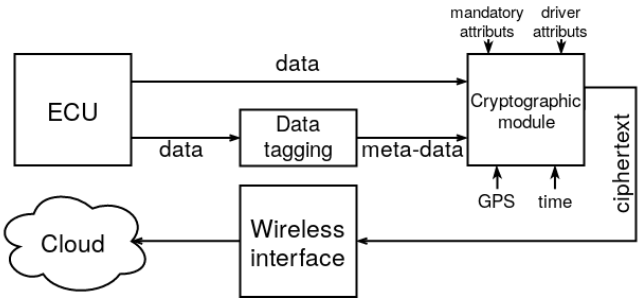

Fig. 2. Vehicle data upload

Figure 2 presents in details data upload to the Cloud (④). Data gathered by sensors are first processed in the Electronic Control Unit (ECU). Then data are tagged with their data type. Using the data and its data type, the user defined attributes and mandatory attributes are selected. The cryptographic module executes the Encrypt algorithm and generates the ciphertext. The ciphertext is sent to the Cloud provider. For security purpose, cryptographic operations are realised in a hardware security module.

Let us come back to the example in section II and illustrate the example with our architecture. The TA runs the System setup phase to initialise the system keys. The car provisioning phase is achieved incorporating the public key into the vehicle and mandatory attributes. Then the company C and the sworn organisation subscribe into the system. C obtains a secret key containing the access tree $gps \wedge C \wedge day \wedge T \wedge low$. The sworn organisation obtains a secret key containing the access tree $T\_vincinity$. During work hours, U's vehicle send periodically to the Cloud gps data encrypted with the attributes *gps*, C, *day*, T and $T\_vincinity$. Outside work hours, U's vehicle send gps data encrypted with the attributes $T\_vincinity$. Finally, C pulls the data from the Cloud and can decrypt them only if they were sent during the work hours. The sworn organisation pulls the data only if U is victim of an accident and can decrypt the data only if it was emitted near T and has been sworn in. Any other person cannot decrypt the data.

VI. Conclusion

In modern ITS systems, a multitude of data (some of which may be considered as private by the driver) are emitted by vehicles to be stored in a Cloud and retrieved by various actors, without any possible driver control. In this paper, we propose 1) a fine-grained privacy-centric access control policy of data based on ABE to address this problem, and 2) a security architecture to enforce such a policy.

As future work, we plan to realise a theoretical study of algorithms complexity, in space and time, along with the scalability of the solution. Then we plan to evaluate and compare ABE schemes and group schemes on a real case to identify which is the best scheme in our application. Then we plan to experiment the solution by simulating communication in a network of vehicles and by implementing a prototype. The use of keys leads to the need for a key revocation mechanism, this mechanism will also be considered in our future work. For the moment, in our architecture, any cars can emit data to be stored in the Cloud, we will have to study an authentication mechanism to limit data emission to members of the system.

References

[1] General Data Protection Regulation of 27th April 2016, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, Last access: 8th April 2019.

[2] Facebook Security Breach Exposes Accounts of 50 Million Users, Mike Isaac and Sheera Frenkel, Sept. 28, 2018, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html, Last access: 23th June 2019.

[3] Bethencourt, J., Sahai, A., and Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) (pp. 321-334). IEEE.

[4] Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98). Acm.

[5] Hong, X., Huang, D., Gerla, M., and Cao, Z. (2008, August). SAT: building new trust architecture for vehicular networks. In Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch) (pp. 31-36).

[6] Huang, D., and Verma, M. (2009). ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Networks, 7(8), 1526-1535.

[7] Ruj, S., Nayak, A., and Stojmenovic, I. (2011, July). Improved access control mechanism in vehicular ad hoc networks. In International Conference on Ad-Hoc Networks and Wireless (pp. 191-205). Springer, Berlin, Heidelberg.

[8] Yeh, L. Y., Chen, Y. C., and Huang, J. L. (2011). ABACS: An attribute-based access control system for emergency services over vehicular ad hoc networks. IEEE Journal on Selected Areas in Communications, 29(3), 630-643.

[9] Liu, X., Xia, Y., Chen, W., Xiang, Y., Hassan, M. M., and Alelaiwi, A. (2016). SEMD: Secure and efficient message dissemination with policy enforcement in VANET. Journal of Computer and System Sciences, 82(8), 1316-1328.

[10] Safi, Q. G. K., Luo, S., Wei, C., Pan, L., and Yan, G. (2018). Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs. Computer standards and interfaces, 56, 107-115.

[11] Chen, N., Gerla, M., Huang, D., and Hong, X. (2010, June). Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption. In 2010 The 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net) (pp. 1-8). IEEE.

[12] Rao, Y. S., and Dutta, R. (2012, December). Computationally efficient secure access control for vehicular ad hoc networks. In International Conference on Information Systems Security (pp. 294-309). Springer, Berlin, Heidelberg.

[13] Nkenyereye, L., Tama, B. A., Park, Y., and Rhee, K. H. (2015). A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control for VANETs. JoWUA, 6(2), 98-112.

[14] Zhang, W., Jiang, S., Zhu, X., and Wang, Y. (2016). Cooperative downloading with privacy preservation and access control for value-added services in VANETs. International Journal of Grid and Utility Computing, 7(1), 50-60.