




Article

Physical Security for Fleet Management Systems

Emad Hamadaqa *, Ayoub Mars  and Wael Adi

Institute of Computer and Network Engineering, Technical University of Braunschweig, Hans-Sommer Str. 66, D-38106 Braunschweig, Germany; a.mars@tu-bs.de (A.M.); w.adi@tu-bs.de (W.A.)

* Correspondence: e.hamadaqa@tu-bs.de; Tel.: +49-176-37665555

Received: 18 November 2019; Accepted: 20 December 2019; Published: 31 December 2019



Abstract: Fleet Management (FM) deals with the management of transport, distribution, and logistics of national and international goods exchange, in which many operators worldwide are involved. Fleet management involves many security-relevant participating entities, such as vehicles, FM mobile clients, smart trackers with goods, drivers, etc. Existing automated fleet management systems are basically vulnerable to physical replacement attacks when managed by mass-produced electronic identities. Analog Physical Unclonable Functions (PUFs) failed to serve as unclonable electronic identities due to being costly, unstable and inefficient for such mass-usage. We propose in this paper to deploy the Secret Unknown Ciphers (SUCs) techniques introduced a decade ago as digital low-cost clone-resistant identities to be embedded in selected participating electronic Fleet Management System (FMS) units. SUCs, as stable self-created digital modules to be embedded in future smart non-volatile (NV)-FPGA devices, are expected to cover all emerging FMS physical security requirements. Such information-retaining units (when switched-off) are emerging to become widely used as ultra-low-power mass-products in automotive environment. We propose a new FMS security architecture based on embedding SUC modules in each security-relevant entity in the FMS such as vehicles, mobile clients, smart trackers and goods. This paper investigates the expected technical impacts when using SUCs technology as physical security anchors in a standard FMS configuration. Several SUC-related generic security protocols adapted to the FM environment show how to securely-link tracing of goods, tracks routing, and personnel in such FM system. It is also shown how to combine other biometric fingerprints to simplify personal liability and enhance the security management in such globally-operating automated procedures. The presented security analysis of the resulting FMS shows that the major security concerns in existing FMSs can be resolved. One major advantage of SUC technique, is that device-manufacturers can be largely-excluded as security players. The FPGA technology required for the SUC solution is currently not available and is thought for future use. The concept is ultimately applicable if the future electronic mass products would deploy self-reconfiguring non-volatile (flash-based) System on Chip smart units. Such units are expected to dominate future Internet of Things (IoT) ultra-low-energy applications, as power-off does not lose any information. The proposed SUC strategy is highly flexible, scalable, and applicable to cover a large class of globally operating protection mechanisms similar to those of the addressed FMS scenarios.

Keywords: fleet management; vehicular security; vehicle tracker; clone-resistant entities; secured electronic logging device

1. Introduction

Nowadays, the need to monitor goods transport and deployed vehicles during their activities is growing as globalized goods exchange is growing worldwide. Fleet operators require secured and precise information about their vehicles and goods traffic such as compliance reporting, International

Fuel Tax Agreement (IFTA), International Registration Plan (IRP), and pre/post-inspections reports [1]. Vehicles can operate globally in various locations in large numbers and for different purposes. On the client side, much information is required in real time between Fleet Management System (FMS) operators' clients, drivers, etc. to fulfill the technology requirements of a distribution process correctly. Contemporary Fleet Management (FM) systems are deploying the global positioning system (GPS) and global system for mobile communication (GSM) technology as standard network services usable for FMSs. Utilizing GSM technology has become popular due to its low cost, and it is an easy way of transferring data with high reliability on existing infrastructure [2]. The Global Positioning System (GPS) is commonly used as a global navigation satellite system to provide location and time information anywhere on Earth. Both systems are very efficient means for tracking, routing, and real-time FM [3,4].

Recently, several security solutions and tracking systems were designed to assist corporations deploying large number of vehicles [5,6]. A Fleet Management System (FMS) is required to optimize the cost and effort required from employees and infrastructure to accomplish the whole process efficiently within minimal times. Additionally, assignments can be scheduled in advance based on tracing vehicles locations. Therefore, central fleet management is essential for large enterprises to meet the varying and growing requirements of customers and to improve productivity. However, the current solutions [5,6] do not secure all FMS entities (driver, vehicle, mobile, goods) sufficiently, and the open communication paths are making the system vulnerable to wide spectrum of attacks [7]. Such geographically distributed system offers large areas of security gaps like the injection of falsified data and especially, faking position information of vehicles and goods. Misbehavior in terms of wrong position information is very likely to disturb the whole system [8]. For example, displacement of operation-relevant mobile device to wrong vehicles by an adversary may disturb the FM process and abuse the whole system. In addition, even by adding an authentication process to the FM mobile, it is still possible to fake the vehicle identification number. Recently, a new FMS era begins with the use of smart pallets [9], low-cost tracker which can detect its own position, as well as being able to track any movements, impacts, and operational condition. For example, networked waterproof sensor detects impacts, inclination, and the acceleration forces on each pallet to improve the quality of transport and tracking [9].

However, all the above solutions suffer from the missing unclonability of the deployed electronic units as GPS and GSM units. Our work focuses on converting electronic units into hard to clone (non-replaceable) entities to act as physical security anchors in a solid fashion. We propose to embed a low-cost and consistent digital clone-resistant technology, coined as Secret Unknown Ciphers (SUC), in some future FMS entities as unclonable structures to serve as security anchors for the FMSs operating on open and global networks. Additionally, we propose to combine SUC with some biometric fingerprint to enhance serving personal identification and liability as in [10]. Combining both technologies allows to build strong authentication mechanisms and attain undeniable transactions for liability issues in FMS processes. The proposed security levels are scalable and even capable to cope with future post-quantum security requirements.

Contributions: this work has the following three contributions, (1) we introduce a new secured Fleet Management System security architecture which deploys clone-resistant physical entities as security anchors in future non-volatile smart electronic units. All relevant fleet management entities should become physically hard to clone/replace. For example, FM involved mobiles, vehicle, and goods-carriers are made physically unique using a new concept of the digital Secret Unknown Ciphers (SUCs) embedded in the participating units. (2) Related generic security protocols to cope with the SUCs in FMS environment are introduced to show the impact of SUC usage on the FM system operation. (3) The techniques are shown to efficiently prohibit any replacement attacks on FMSs at adequate cost and complexity. A security analysis is provided to shows that the resulting system is highly secure and resilient.

The remainder of this paper is organized as follows. In Section 2, we investigate related works that have been introduced on vehicular networks security and current FMS architecture. Current FMS system architecture, possible attacks on that system, and our proposed enhancing security requirements

are presented in Section 3. In Section 4, the targeted secured necessary FMS architecture is presented. Generic new identity creation using SUC technology together with the corresponding protocols are presented in Section 5. Multi-Realm Operational Capability are presented in Section 6. Security analysis of the proposed FMS against a variety of attack scenarios is presented in Section 7. Section 8 concludes the attained results and presents possible future works.

2. Related Work on the Security of FM Systems

Vehicle tracking systems are widely used in different sectors such as smart traffic management systems, vehicle location tracking systems, anti-theft vehicle tracking systems, parking management systems, fleet management, and in the field of Intelligent Transportation Systems (ITS) or Smart Transportation Systems (STS). This section presents some selected state of the art FMS systems from the open literature.

In [11] the authors propose a cloud-based fleet management platform through integrating the advantages of Internet of Things (IoT) and cloud technology but the security and privacy issues have not been well addressed. In [12], an Automatic Vehicle Monitoring (AVM) platform was proposed, it manage multiple heterogeneous devices for fleet management, monitors street traffic and supplies high-level services. This platform provides a monitoring service for several properties in the vehicle, which can be read over an On-Board Equipment (OBE) device. However, the authors choose GPRS as a communication network that has great limitations of range, data rate, and availability. In [13], authors proposed a dynamic FMS with an event-based architecture. The system changes the task management workflow of the fleet entities. They applied this architecture to the coordination of a fleet of ambulances in a medical emergency scenario and show experimentally that the proposal outperforms a nondynamic approach. In [14], Gowda et al. proposed a system to provide effective vehicle tracking, real-time monitoring. The real-time vehicle fleet management and Security System has an in-vehicle system in which all the hardware is interfaced to a Cubie Truck board. This in-vehicle system is placed in the vehicle. A remote server used for data acquisition in real-time and graphical user interface is created for user interface and dynamic plotting. However, the authors do not provide any security analysis for their security system. Malekian et al. described the design and development of a wireless On-Board Diagnostic II (OBD II) fleet management system. The system measures vehicle speed, distance, and fuel for tracking and analysis purposes [15]. The use of the OBD II port to obtain vehicle operation data was an important aspect of this work because this port is featured in the vast majority of current vehicles.

Recently, many FMSs have been proposed, designed, and implemented with smart services. The FMS tracking services and other functionalities are provided to users [5]. Other systems provide additional functionalities besides tracking such as allowing users to search for addresses and directions, and historical playback for vehicles' movement [6]. Other services provide a desktop application which provides distance calculations in addition to the basic tracking system [16].

All the currently provided solutions use just basic user password authentication mechanism to access the web portal or the mobile application. Therefore, all these systems suffer from being very weak in clonability resistance leading to be easily exposed to many replacement-attacks and abuse scenarios especially in future automated globally operating smart FMSs.

3. Modern Operational FMS Architectures

Transport and logistics companies maintaining a fleet of vehicles and trailers for transport of goods need efficient management for their vehicles using fleet management information systems. In the following, a standard sample FMS architecture is depicted as a model to project our proposed security architectures on-to it.

3.1. Sample Modern FM Functional System Architecture

Figure 1 describes a sample modern FMS architecture; a vehicle with an integrated GPS receiver for routing and tracking, a mobile device with installed Fleet Management Client (FMC) application

connects to the vehicle Electronic Control Unit (ECU) via OBD II [15], the FMC reads vehicle data like speed, fuel, Mass Air Flow (MAF) and sends the data wirelessly to the fleet management backend server, where the data is stored and processed in various components.

Drivers use the FMC application on their mobile device to login into the FMS, and authenticate themselves with username and password. In the case of successful authentication, the login session will open. The FMC application automatically calculates IRP and IFTA miles-per-state using the GPS data. Drivers can enter information into the FMC application for supporting documents such as fuel purchases, tolls, and meals as well as their pre- and post-trip inspections. This data, along with the duty log, IFTA, IRP, and inspection data, creates a complete trip record that can be viewed, audited, archived, and printed from Fleet Manager (FM). In the truck box or trailer, the low-cost Smart Tracker (ST) enables load carriers (pallets) to connect to the FMS; an ST contains a GPS receiver and is connected to the mobile data network using SIM cards. Each ST sends the current position to the FMS frequently [17,18].

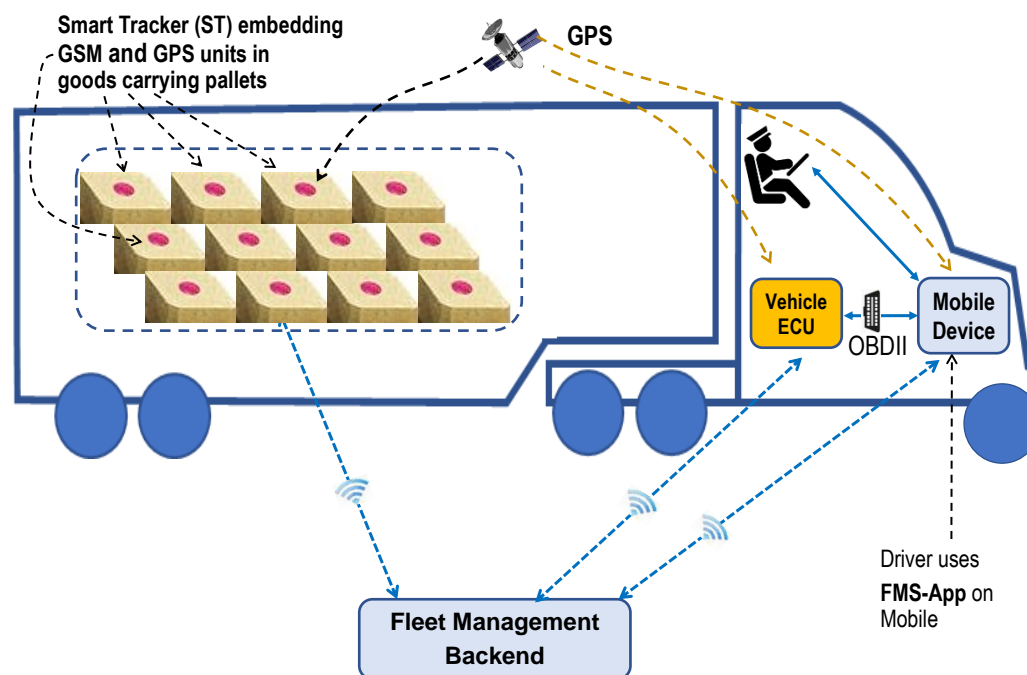


Figure 1. Sample typical modern fleet management system architecture.

3.2. Threat Models and FM-Adversary Types

Securing the FMS requires first identifying possible attacks scenarios, their nature, and their capacity to damage the system. The possible attacker types could be categorized into [19]:

- Insider and Outsider: insiders are the authenticated users of FMS, whereas outsiders have a limited capacity to attack.
- Malicious and Rational: malicious attackers have no personal benefits to gain from an attack; they just harm the functionality of the network. Rational attackers have a personal profit motive.
- Active and Passive: active attackers generate or modify messages, whereas passive attackers only read the traffic.

3.3. Assumed Attack Scenarios on Existing FMS

Due to the open wireless nature of FMS and route information efficiency requirements from source to destination, there are many types of attacks that can hamper the successful deployment and execution of FMSs [20]:

1. **Impersonation Attack:** in this attack, an adversary takes over the identity and privileges of an authorized FMS entity. Active adversaries perform this type of attack. They may be insiders or outsiders. This attack is a multilayer attack, i.e., an attacker can exploit either network layer, application layer or transport layer vulnerabilities. An attacker steals property of the legitimate user; the attacker can claim that it is a genuine user. By using this type of attack, a fake mobile can claim that it is an FMS mobile to send wrong positions to the FMS. Figure 2 shows four sample different types of impersonation attacks on FMS:

- Attack 1: an adversary impersonates the mobile
- Attack 2: an adversary impersonates the vehicle
- Attack 3: an adversary impersonates the ST.
- Attack 4: an adversary impersonates the driver.

As FMS entities do not currently have physically secured identities, an adversary may basically counterfeit the identities of the vehicle and mobile. Also, the adversary can replace real goods with fake goods, and can exchange corrupted data such as the GEO Location, speeds, etc. with the FMS.

2. **Location Tracking Attacks:** the current FMS entity position or the path followed along a period can be used to track the vehicle, mobile, smart tracker, and obtain information about drivers.
3. **Eavesdropping Attacks:** this attack belongs to the network layer attack and passive categories. The main goal of this attack is to access confidential FMS data.
4. **Denial of Service (DoS) Attacks:** in DoS attacks, the main objective of the attacker is to disturb the communication channel or overwhelm the FMS's services available to legitimate users and entities. This attack makes the system useless. In this way, critical information cannot be conveyed to vehicles on time. Moreover, it can cause or increase the danger to the driver if she/he depends on the application's information to make decisions. For example, an attacker floods the gateway service with traffic (wrong messages) in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them. The gateway service is the point of standardized public communications; this makes it a perfect target for a DoS attack.

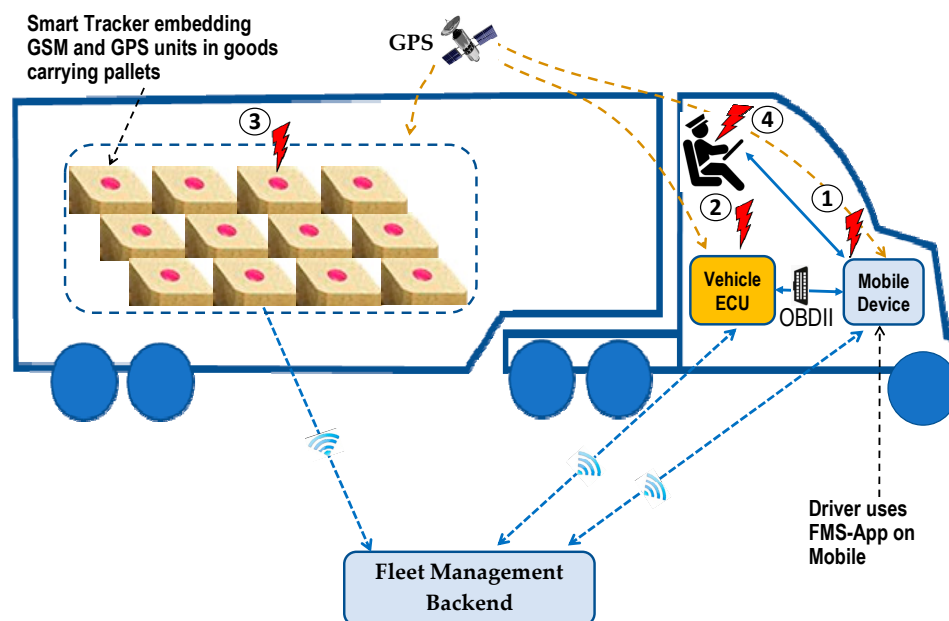


Figure 2. Threat and attacks model on current fleet management systems.

In all known state-of-the-art treatments, no physical security is involved in making physical units unreplaceable. Hence, there is a need for a solution that can securely identify clone-resistant vehicles, mobiles, goods, and drivers. This identification should be made in real-time to attain stable security anchors for contemporary FMSs. More security requirements are therefore necessary.

3.4. Proposed Enhanced Security Requirements for Future FMS

In this Section, we propose new and additional set of security requirements to counteract expected future threats:

- **Individual physical entity authentication:** each security-relevant entity such as mobile, vehicle, smart tracker, and driver should become individually identifiable to the FMS backend at any time.
- **Jointly physically clone-resistant entities:** in order to counteract the significant severe attacks on fleet management, all relevant entities should be capable of being jointly unreplaceable. For example, an inseparable secured individual pairing of “mobile/vehicle is necessary. Under this requirement, no replacements or impersonation attacks such as attack 1 and attack 2 would be possible.
- **Location certainty:** the FM entities are required to deliver strictly authentic and unclonable geo-positioning to the FMS to counteract false or fake routing.
- **Unclonable time scale:** one of the primary system requirements is that the FMS should process all real-time information which is consistent and not possible to fake.
- **Non-repudiation:** requirement assures that it will be impossible for an entity to deny having sent or received a message.
- **Exclusive confidentiality of relevant information:** the FM communications should only allow information to reach the dedicated authorized parties.
- **Availability:** implies that every mobile/vehicle or any relevant entity should be capable of delivering information and acting authentically at any necessary time. The Denial-of-Service (DoS) attack should be prevented or at least securely detected.
- **Data integrity and authenticity:** delivered data messages should not be modifiable and, more importantly, should be authentic; this also implies that the received information is fresh. False or modified data should not lead to potential system crashes, bottlenecks, and other problems.

4. Proposed New Low Energy Highly Secured FM Structures

One fundamental primitive remedy for the majority of the above requirements is the deployment of clone-resistant functions or identities for all relevant entities including mobile, vehicle, driver, goods, etc. The FMS is required to integrate unclonable and tamperproof identities into each entity and linking them with the FMS security architecture such that any attempt to abuse/fake any physical or geographical information would be securely identified in real-time by the FMS management.

4.1. Proposed New Clone-Resistant Modules for FMS Components

To fulfill the security requirements described above, each FMS component (vehicle, mobile device, and smart tracker) should embed its unique clone-resistant functions. In addition to that, drivers will be identified by their unique biometric keys. In this way, strong authentication between the FMS components would be ensured.

4.1.1. Clone-Resistant Module for FM Electronic Entities

Physical Unclonable Functions (PUF) have been proposed as unclonable structures to make electronic units physically non-replaceable in the last two decades [21–23]. PUFs deploy many intrinsic device properties to extract provable devices DNA-like identities. Due to the PUFs analog nature, PUFs have inconsistent responses when challenged under different environmental conditions or in different times because of aging effect. Fuzzy extractors were proposed to stabilize PUFs behavior [24,25].

However, such error correction mechanisms have high hardware/software complexity and reduce the system entropy.

To overcome PUFs limitations, new digital (non-analog) clone-resistant function coined as Secret Unknown Cipher (SUC) was proposed in [26–29]. SUC is a random, unpredictable, and unknown internally self-generated cipher created inside each chip, such that no other party, even the manufacturer, may back trace the generated cipher inside the chip. As digital structure, each resulting SUC inside a chip is robust and consistent during the whole chip's lifetime.

In this work, we propose to deploy such SUCs as clone-resistant modules without participating the device manufacturer in all future security-relevant FMS electronic component. Our solution is to integrate unclonable and tamperproof identities into each individual entity and link them such that any attempt of physical or geographical separation would be securely identified in real-time by the FMS. FM entities (mobile, vehicle ECU, smart tracker) are produced by different manufacturers.

The Concept of SUC: As SUC concept is not well known in the public literature, we introduce the concept again to make the paper self-contained. Figure 3 describes the concept for embedding SUC in System on Chip (SoC) units that are based on self-reconfiguring non-volatile SoC FPGAs. The SoC FPGA should reside in the main chip/unit of each FMS component (mobile, vehicle ECU, smart tracker). The Trusted Authority TA responsible for triggering the creation of the SUCs could be even the FMS manager without participating the device manufacturers.

Notice: We assume that such smart non-volatile devices would dominate the future electronic IoT devices for many reasons. The major reason is that non-volatile technology is an essential requirement for ultra-low-power systems as full power-off do not lose any processed information.

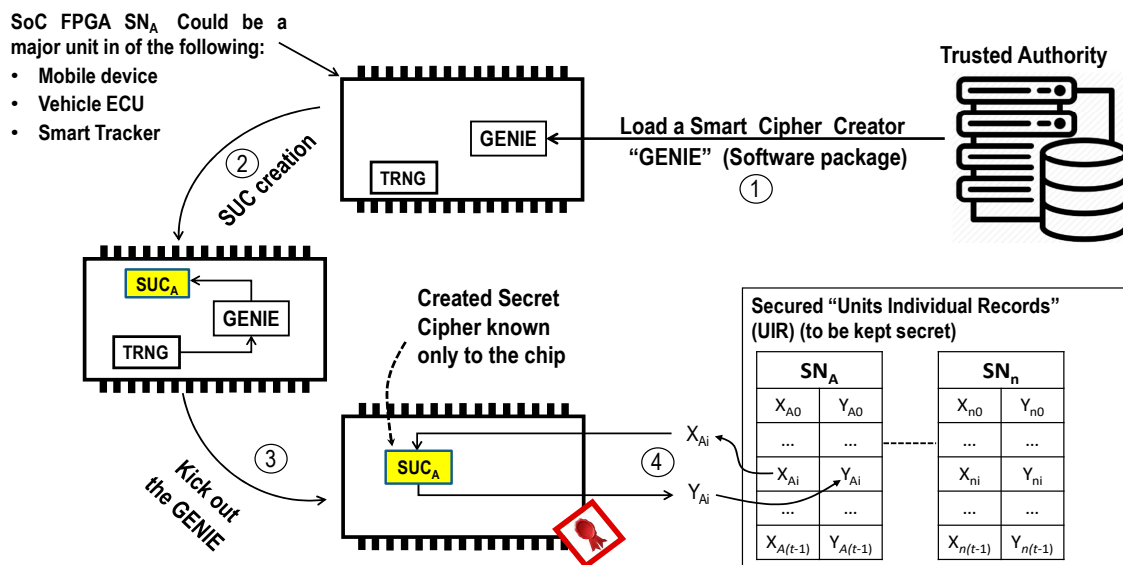


Figure 3. Secret Unknown Cipher (SUC)-enabled central control units for mobile and vehicle as unclonable module.

The personalization process by TA on each SoC FPGA may proceeds as follows:

- **Step 1:** TA injects a software package called "GENIE" into each unit that contains an algorithm for creating internally unpredictable and unknown random secure ciphers. The TA injects the GENIE for a short time into each SoC unit to run just one time and never again.

- **Step 2:** The GENIE creates then a permanent (non-volatile) and unpredictable random cipher by deploying random bit's string from an internal and unpredictable True Random Number Generator (TRNG).
- **Step 3:** When the GENIE completes the creation of the SUC, it will be fully deleted and the SoC unit ends up with its unique and unpredictable SUC.
- **Step 4:** The TA challenges the SUC_A using a set of clear text challenges $X_A = \{X_{A,0}, X_{A,1}, \dots, X_{A,t-1}\}$ and receives the corresponding cipher text responses $Y_A = \{Y_{A,0}, Y_{A,1}, \dots, Y_{A,t-1}\}$. It stores them on the corresponding area in its secure "Units Individual Records" (UIR) defined by the Serial Number of the device (SN_A). In [26], an efficient mythology to manage X/Y pairs was proposed; the set of challenges X_A can be generated by deploying a seed S_0 such that: $X_{A,i} = S_0 + i$ for $0 \leq i \leq t-1$. This reduces the memory complexity required to store X/Y pairs in the participating devices of the FMS.

Notice: TA may be any trusted authority assigned by the FMS or the FM administrator himself. The device manufacturer is just offering devices and has no information about the GENIE or the personalization process. The devices can be irreversibly locked after the above 4 step personalization process and may never be changed again.

Generic Physical Identification Protocol for SUC Units: a fleet manager having unit A's set of X/Y individual records can authenticate unit A according to the sample following protocol.

In reference to Figure 4, a two-way protocol can be used by an FMS to identify a physical unit A (SN_A), having SUC_A and SUC_A^{-1} structures as follows:

- TA selects randomly one of the $X_{A,i}/Y_{A,i}$ pairs and challenges unit A with $Y_{A,i}$. Unit A uses its SUC_A^{-1} to decrypt $Y_{A,i}$ resulting with the corresponding cleartext $X'_{A,i} = SUC_A^{-1}(Y_{A,i})$ and sends $X'_{A,i}$ to TA.
- If $X_{A,i} = X'_{A,i}$, then the unit is deemed to be authentic and can be accepted. Otherwise, unit A is not authentic and should be rejected. The pair $X_{A,i}/Y_{A,i}$ is marked as consumed and should not be used later for highest security performance.

Compared to PUFs, SUC has the advantage that it is capable to recover X from Y by using the inverse function SUC^{-1} . This property allows low-complexity and very efficient management of the consumed X/Y-pairs. The property was also used in [30] to build a physical chain of trust for a secured over the air vehicular software update.

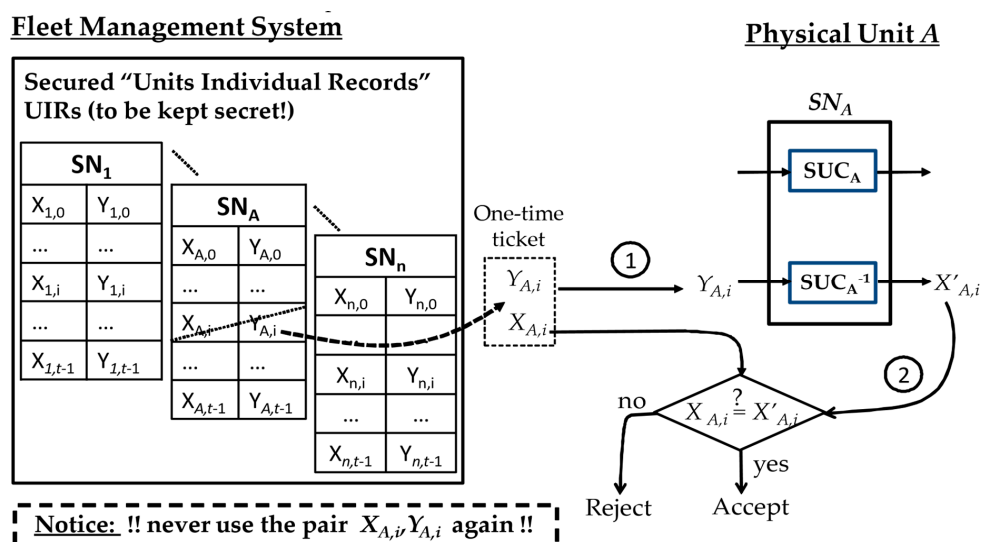


Figure 4. Generic use protocol for a Secret Unknown Cipher (SUC).

4.1.2. Combining Biometric Fingerprints as Additional Security Enhancement

The biometric fingerprint is a personal authentication technique based on an individual's polar fingerprint. Fingerprint authentication techniques have little possibility of being attacked by someone who does not have access to privacy data. It allows people to verify themselves using a simple process, by putting their fingerprint into the fingerprint scanner. This technique is assumed to be better than authentication technologies such as passwords, PIN, or tokens that require people to remember multiple words and numbers but still vulnerable. Various biometric-based systems for remote user authentication have been suggested as summarized in [31–33] summarize a good representative selection.

To ensure the security of the driver's fingerprint in the FMS, we propose a combination of SUC technology (unclonable mobile physical identity) and the operating system Fingerprint API (mobile fingerprints reflecting driver identity) for FMS authentication process.

4.2. Proposed FMS Security Architecture

Figure 5 illustrates a sample embodiment of the SUC security enhancement scenario in the mobile, vehicle and smart trackers to create an identity which cannot be faked or replaced without the strict knowledge and administration of the FMS. Vehicle ECU provides a gateway for the smart trackers, which frequently sends its position over the gateway to the mobile device FMS backend. In this way, the ECU builds a low energy wireless local network area for all STs so that STs never use GSM communication during a trip. The mobile fingerprint sensor for user identification will be used to build a biometric identity to identify drivers. Biometrics verifies that the person boarding the vehicle is a verified driver that is trying to access the FMS mobile application by comparing the entered characteristic inputs and registered characteristic inputs which are extracted from unique and highly discriminatory characteristics. To fulfill the location certainty requirement, the FMS determines the current position of the vehicle, mobile, and loaded STs. On the FMS backend, a position agent analyses the trip location data, which contains mobile, vehicle, and ST position data and generates violation events if different positions are detected for the three entities.

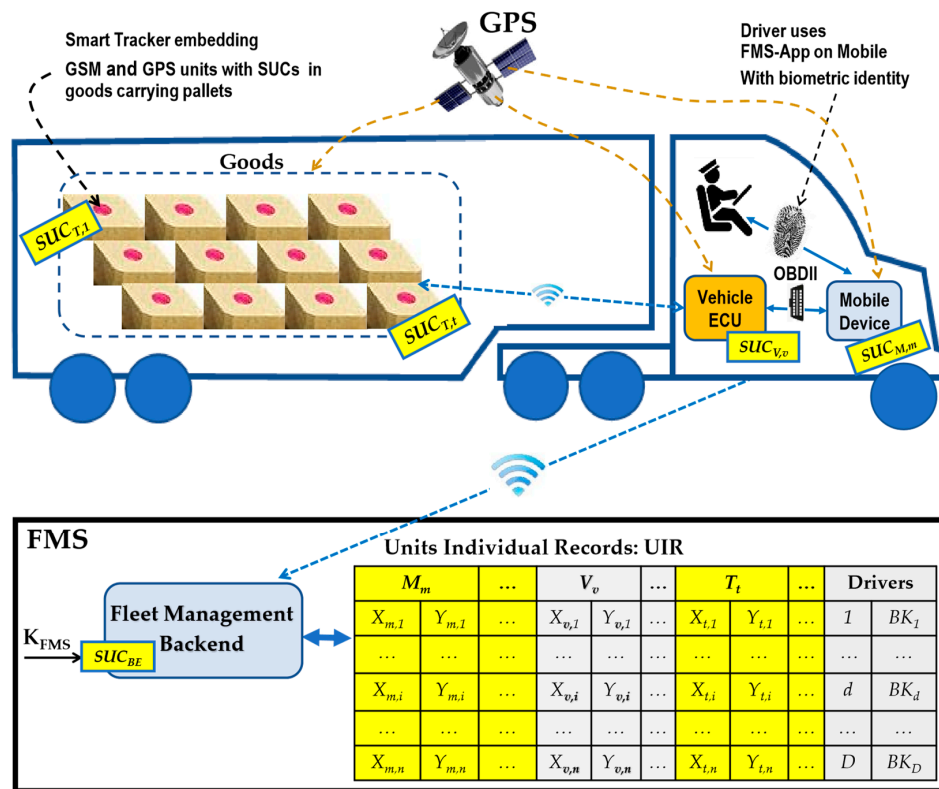


Figure 5. Sample integration of proposed unclonable identities into Fleet Management System (FMS) entities.

The following sample added SUC embodiments are proposed to be integrated in some FMS units to fulfill the enhanced security requirements in the proposed FMS security architecture:

4.2.1. Clone-Resistant Vehicle ECU

The SUC is embedded in a customized Electronic Control Unit (ECU) in the vehicle. ECU captures rich data on vehicle position, speed, fuel use, idling, and more, and communicates directly with the FM mobile device over the OBD II interface. Integrating SUC into the vehicle increases vehicle security and makes ECU clone resistant. A mutually hard-to-clone authentication between vehicle and mobile device can be strictly and securely achieved.

4.2.2. Clone-Resistant Mobile Device

The FM mobile application runs on the mobile device with integrated SUC; The FM mobile application security module provides the necessary security-relevant functions such as encryption, decryption, generation, and verification of cryptographic keys. Clearly, a hardware solution provides higher performance and a far higher security level. In this proposal, security protocols described in Section 5 will be implemented in the FM mobile application. The FM mobile application is added as a form of Software Developer Kit (SDK) that is installed in the mobile device. It is the communication interface with the Fleet Management backend services. It encapsulates the implementation of the transfer protocol to the FM backend system. All known fleet management processes like driver management, vehicle management, map functionalities, compliance, dispatch and order, messaging, etc. are to be implemented in the FM mobile application.

4.2.3. Clone-Resistant Smart Tracker and Goods

The state of the art Smart Tracker (ST) [9] presents an alternative goods tracking system based on GSM networks. A complete GPS receiver was integrated and latitude and longitude coordinates were

sent to the FMS via SIM card. The device can detect its position and it is able to track any movements, impacts, and changes in temperature and weight. The ST reports its status whenever there is a deviation from the plan, e.g., if it senses an unexpected shaking or temperature fluctuations. ST passes its data updates automatically back to the FMS backend. Our solution is proposing to integrate a SUC into each ST offering a very efficient clone-resistant identification and management capabilities and makes the STs less vulnerable to cloning attacks. A physically hard-to-clone authenticated chain between ST and the vehicle's ECU or possibly other units can be strictly and securely established.

4.2.4. FM Backend Server with Physical SUC Security

The FMS Backend Server with embedded SUC provides necessary services for client applications. These services help to distinguish between the different types of component tasks, making it easier to create a design that supports component reusability. Each service contains several discrete component types grouped into sub-layers, with each sub-layer performing a specific task. The core services are "fleet management service, user services, platform service, compliance service, gateway service, and trusted authority service. Trusted authority service is introduced to the FMS Backend with the primary task identification of FMS entities (driver, vehicle, mobile, and smart tracker) and controlling their access to the fleet management Backend Services. The trusted authority service stores encrypted secret records for each entity for later usage. Each SUC has its pair records, as shown in Figure 5. Trusted authority service uses backend server SUC-Hard-Token (SUC_{BE}) with the key K_{FMS} to physically secure the encryption and decryption of FMS messages.

5. SUC-Related Security Enhancement Protocols

This section addresses basic sample generic protocols to conduct the required operations in the SUC-based proposed FMS. The following notations are used in the protocols below:

- Smart tracker T_t possesses $SUC_{T,t}$ and has a position P_T with its timestamp TS_T
- Vehicle V_v possesses $SUC_{V,v}$ and has a position P_V with its timestamp TS_V .
- Mobile M_m possesses $SUC_{M,m}$ and has a position P_M with its timestamp TS_M .

5.1. Overview on the System Security Workflow

The fleet manager manages all FMS entities (vehicle, mobile, smart tracker, and driver). When a fleet manager inserts a new entity in the FMS, the enrollment process for this entity should be executed as follows: The FMS requests an entity possessing SUC_X to generate challenge-response pairs, then the FMS encrypts the challenge-response pairs using its own SUC_{BE} and private key K_{FMS} and stores them in the FMS entity table.

To manage trips in the FMS, the fleet manager must first assign a mobile phone to the driver, then assign a driver to a vehicle and assign at least one load to the vehicle. Each load includes a minimum of one pallet with integrated smart tracker. Figure 6 shows a sample system workflow.

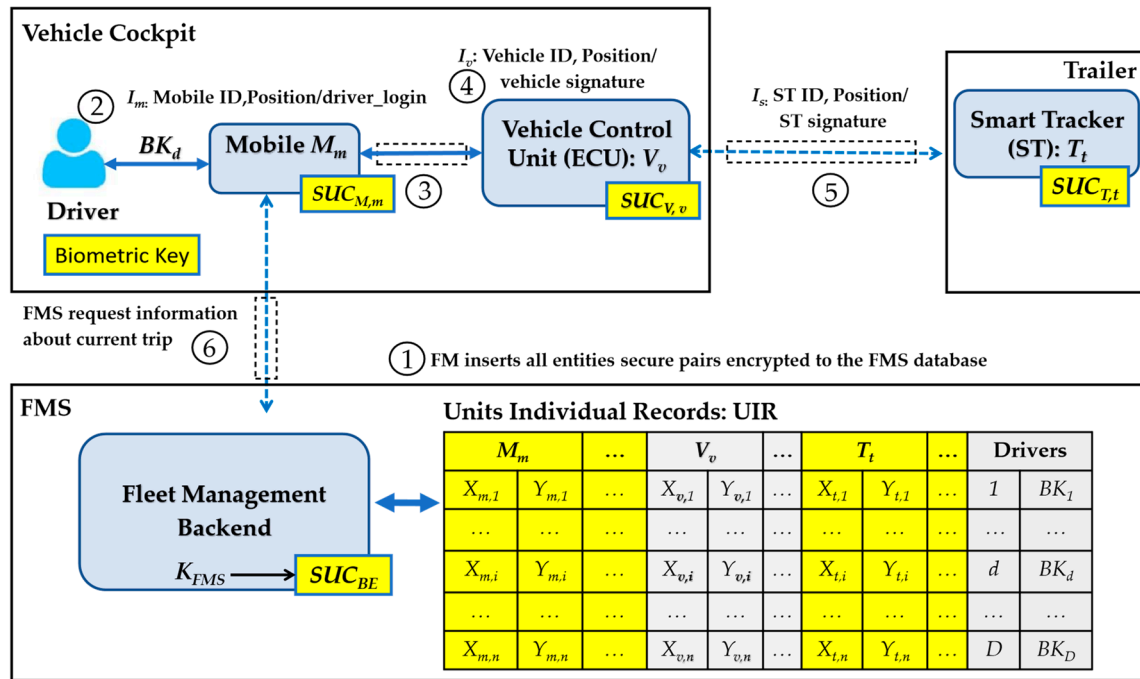


Figure 6. Simplified FMS security actions workflow.

The system workflow scenarios may proceed as follows:

- **Action 1:** The FMS backend server personalizes all FMS entities: a mobile M_m having $SUC_{M,m}$, a vehicle V_v having $SUC_{V,v}$, a smart tracker T_t having $SUC_{T,t}$, and a driver d having a biometric identity BK_d . All records are encrypted by using SUC_{BE} and the personal private key K_{FMS} of the backend operator, that is the records are only accessible if both the physical token SUC_{BE} and the private key K_{FMS} are available.
- **Action 2:** Driver BK_d logs in via fingerprint to start using the FMS client application on the mobile M_m . Mobile M_m sends I_m to FMS.
- **Action 3:** Mutually authenticated M_m and V_v are imitated and presented authentically to FMS backend server. Both M_m and V_v confirm to the server that the other party is not fake.
- **Action 4:** The vehicle V_v sends information I_v via mobile, including an unclonable source-authentication signature for the vehicle and mobile.
- **Action 5:** Smart trackers (ST) T_t sends information I_s via mobile including an unclonable source-authentication signature for the smart tracker, vehicle, and mobile.
- **Action 6:** The FMS requests information about the current trip by sending a message to the FM mobile app.

Any physical separation of M_m , V_v , and T_t is securely forwarded to the FMS in real-time as will be shown in the security protocols in the following sections.

5.2. Owner Enrollment Setup Process for Clone-Resistant Entities

The enrollment process is divided into two parts: management of fleet entities (mobile, vehicle, smart-tracker) which can be done by the fleet manager on the FMS web portal, and driver registration, which can be done on the FM mobile application by the driver.

5.2.1. Enrolling Fleet Management Entities Using SUCs

The enrollment of the FM entities is conducted by a TA assigned by the FMS or the FM administrator himself. As stated before, the device manufacturer has no information about the GENIE

or the personalization process. The TA collects challenge-response pairs from every unit (mobile, vehicle, smart-tracker) and adds these units to the system. Since a vehicle can be used by many drivers and transport different pallets with different smart-trackers, each time the FMS will assign a vehicle to the corresponding mobile, smart trackers, and driver in the trip management module.

5.2.2. Sample Driver Registration Protocol

During the driver registration on the FM mobile application, a driver biometric key will be extracted from the mobile fingerprint sensor using the operating system fingerprint API [34] and sent to the FM backend in combination with the mobile SUC. Trusted authority service stores the biometric key in the FMS driver table after checking the mobile authenticity. Figure 7 describes the executed steps when a driver tries to register (Protocol 1).

Protocol 1: Driver registration protocol

Objective

- Driver registration: The registration process for the driver can be done securely via FMS mobile application.
 - The combination of physical security of the mobile and the driver biometric identity guarantees that the identity of the driver is linked to the identity of the used mobile.
-

Prerequisites

- Mobile device managed by FMS
 - Driver already assigned to FMS mobile device
 - FMS mobile application installed on FMS mobile device
-

Output:

- Successful registration message for registered driver
 - Registration failed message in case of error while register the driver
-

Steps:

1. Mobile M_m obtains the biometric identity of the driver d (BK_d) out of many drivers $\{1, 2 \dots d \dots D\}$ using the operating system fingerprint API [34].
 2. Mobile M_m selects an unused $X_{m,i}/Y_{m,i}$ pair of its $SUC_{M,m}$, then it encrypts BK_d together with $X_{m,i}$ using a standard cipher E , such as AES, and sends it concatenated with the serial number SN_{M_m} of the mobile and $Y_{m,i}$ as: to the FMS. The FMS finds the corresponding challenge $Y_{m,i}$ for $X_{m,i}$ in the UIR corresponding to Mobile M_m ; then it decrypts the received message as $E_{X_{m,i}}^{-1}(E_{X_{m,i}}(BK_d||X_{m,i})) = BK_d||X'_{m,i}$ to obtain the driver's biometric identity. The FMS checks the integrity of the received message from mobile M_m by checking if $X_{m,i} = X'_{m,i}$. The FMS stores the biometric key and sends an acknowledgment ACK together with $X_{m,i}$ encrypted with the same key $X_{m,i}$ to the mobile.
 3. Mobile M_m decrypts the received message from the FMS and checks its integrity. When ACK is valid for the FMS, mobile M_m shows the driver a successful registration message.
-

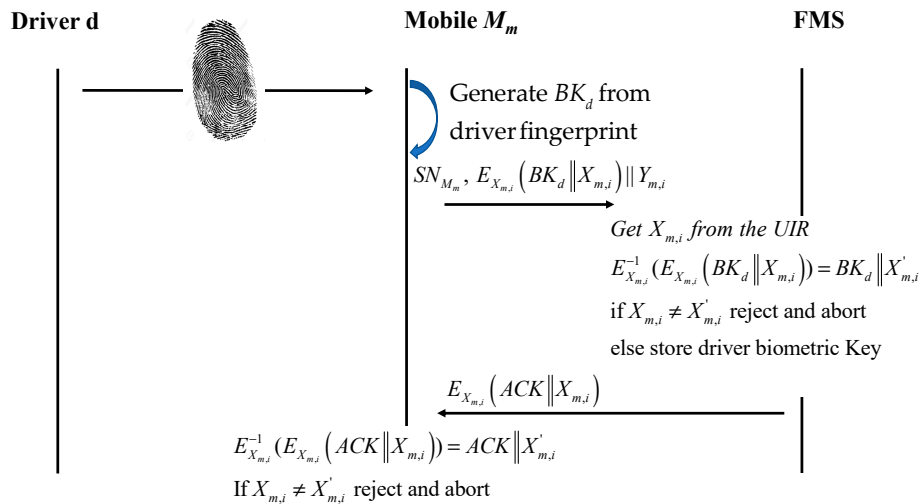


Figure 7. Driver registration protocol.

5.3. Driver Login Protocol

Biometric identity is used to allow only genuine drivers to login to the FM mobile application. The login protocol proceeds similarly to the registration protocol above.

5.4. Driver Actions and System Events Protocol

Driver actions: FMS verifies the genuineness of received data from FMS mobile app.

After successful login, extended user actions are possible, e.g.,

- Set duty status: on-duty, off-duty, and driving
- Driver's vehicle inspection report
- Upload documents such as fuel receipt or hotel receipt
- Reports of electrical or mechanical defects

The same protocol will be used for diagnostic events or violations, which is calculated by the FM mobile application. Figure 8 describes a driver actions and events protocol (Protocol 2).

Protocol 2: Driver actions and system events protocol

Objective:

- Driver actions and system events: Driver actions and system events should be sent securely and in real-time to the FMS backend server.
 - Mobile is physically secured, which prohibits impersonation attack
-

Prerequisites:

- Driver is logged in the FMS mobile application.
-

Output:

- Successful message, mobile application show the driver action sent notification
 - Action failed message in case of error
-

Steps:

1. Mobile M_m sends the encrypted action or event message Q as $SN_{M_m}, E_{X_{m,i}}(Q \| X_{m,i}) \| Y_{m,i}$ to the FMS.
 2. FMS decrypts the received message, checks its integrity, and if the message is valid, the FMS processes the action or event.
 3. FMS sends an encrypted ACK as $E_{X_{m,i}}(ACK \| X_{m,i})$ to the mobile.
-

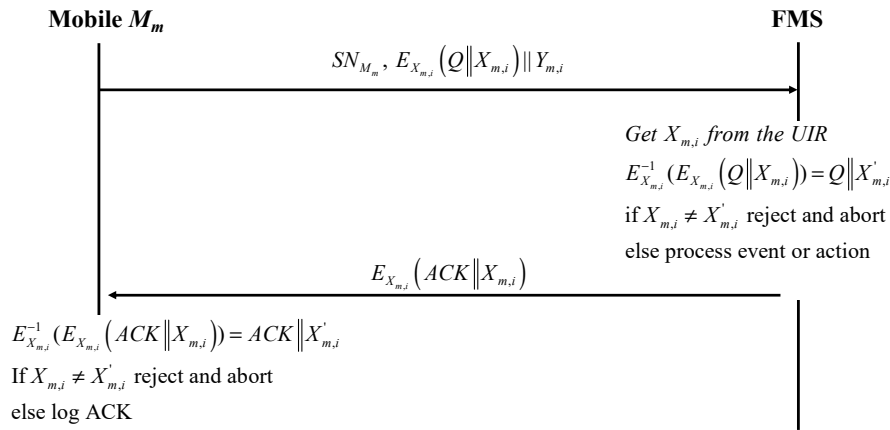


Figure 8. Driver actions and system events protocol.

5.5. FMS-Actions Protocol

The fleet manager monitors drivers, vehicles, and loads via the FMS Web interface; sends load and tours to the driver; and requests a current position from the FM mobile application. Figure 9 describes a protocol for managing FMS actions (Protocol 3).

Protocol 3: FMS actions protocol

Objective:

- FMS actions: Fleet manager or FMS actions should be sent securely and in real-time to the FMS mobile application.
-

Prerequisites:

- Driver is logged in the FMS mobile application.
-

Output:

- Mobile application response will be stored or shown if the action was triggered from FMS user interface.
-

Steps:

1. FMS selects an unused $X_{m,i}/Y_{m,i}$ pair of $SUC_{M,m}$ embedded in a targeted mobile M_m , then it encrypts the request RE together with $X_{m,i}$ and sends it concatenated with $Y_{m,i}$ as: $E_{X_{m,i}}(RE||X_{m,i})||Y_{m,i}$ to Mobile M_m .
 2. The Mobile M_m triggers its $SUC_{M,m}$ with $Y_{m,i}$ to get $X_{m,i}$ and decrypts the message received from FMS. If the decryption was successful, mobile M_m processes the action. Otherwise, it rejects and aborts.
 3. FMS Mobile application sends an encrypted response RS to FMS.
-

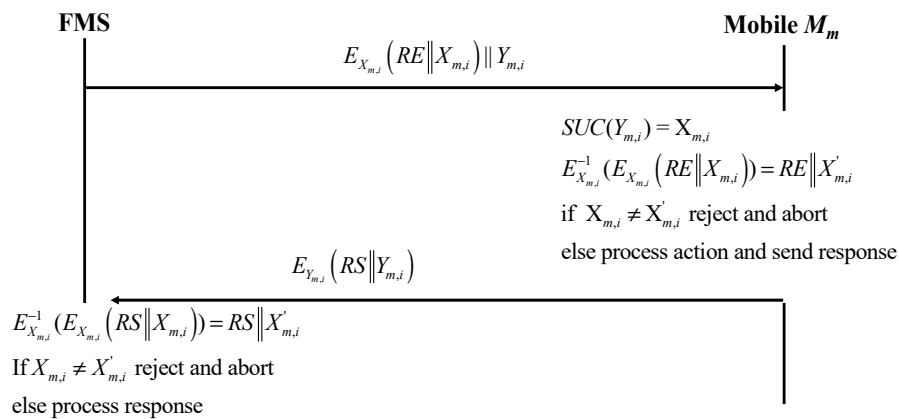


Figure 9. FMS-actions protocol.

5.6. Secured Unclonable and Undeniable Position Tracking

The FMS has always an updated assigning list for each set $F = \{\text{vehicle, mobile, smart tracker}\}$.

Each set F should send its position including timestamps frequently to the FMS. We assume here that the mobile is responsible for contacting the FMS to reduce the traffic and ensure low power consumption by the smart trackers. Figure 10 describes a secured unclonable and undeniable position tracking protocol (Protocol 4).

Protocol 4: Position tracking protocol

Objective:

- FMS entities: FMS entities send position and additional properties securely and in real-time to the FMS backend server.
 - Genuineness of all fleet management entities: mobile M_m , vehicle V_v and smart tracker T_t are ensured by physical security.
-

Prerequisites:

- Driver is logged in the FMS mobile application.
-

Output:

- Mobile application's response will be stored or shown if the action was triggered from FMS user interface.
-

Steps:

1. The smart tracker T_t selects randomly one of the unused tickets pointed to by an index i . Then, it encrypts its position P_T with its timestamp TS_T as $E_{Y_{t,i}}(P_T, TS_T \| X_{t,i})$ and sends it concatenated with its serial number $SN_{T,t}$ and i . This would allow the fleet management system to check the integrity of the received message in addition to validating that it comes from a genuine smart tracker. $SN_{T,t}$ and i allow the FMS to find directly the used CRP in the corresponding UIR of the smart tracker T_t .
 2. Vehicle V_v selects randomly one of its unused tickets pointed to by an index j . It encrypts the received message from the smart tracker $T_t(Q_1)$, then it generates $Q_2 = \{SN_{V,v}, E_{Y_{v,j}}(P_V, TS_V \| Q_1 \| X_{v,j}) \| j\}$ and sends it to mobile M_m . $SN_{V,v}$ and j allow the FMS to find the used CRP by vehicle V_v .
 3. Mobile M_m selects randomly one of its unused tickets pointed to by an index k . It encrypts the message received from vehicle $V_v(Q_2)$, then it generates $Q_3 = \{SN_{M,m}, E_{Y_{m,k}}(P_M, TS_M \| Q_2 \| X_{m,k}) \| k\}$ and sends it to the FMS. $SN_{M,m}$ and k allow the FMS to find precisely the used CRP by mobile M_m .
 4. The FMS picks the response with index k ($Y_{m,k}$) from the UIR corresponding to Mobile M_m serial number $SN_{M,m}$. Then it decrypts the message received from M_m and checks its integrity by verifying that $X_{m,k} = X'_{m,k'}$ if not the FMS rejects and aborts the communication. Otherwise, it obtains picks the response with index j ($Y_{v,j}$) from vehicle V_v UIR and decrypts Q_2 . The FMS checks the integrity of this message by comparing $X_{v,j}$ to $X'_{v,j'}$ if not equal it rejects and aborts the communication. Otherwise, the FMS gets the response indexed with i ($Y_{s,i}$) from the smart tracker T_t UIR and decrypts Q_1 . The integrity check is passed if $X_{s,i} = X'_{s,i}$. At this stage, it is proven to the FMS that the received query (Q_3) from mobile M_m passed all the chain starting from the smart tracker T_t , and no entity can deny its participation in building this query (Q_3). The FMS can compare the received positions P_T , P_V and P_M from the smart tracker, vehicle and mobile respectively. If the positions are close to each other, then the FMS can be sure that all entities exist in the same place.
 5. The FMS sends back a success acknowledgement for receiving position data.
 6. The smart tracker T_t verifies the acknowledgement.
-

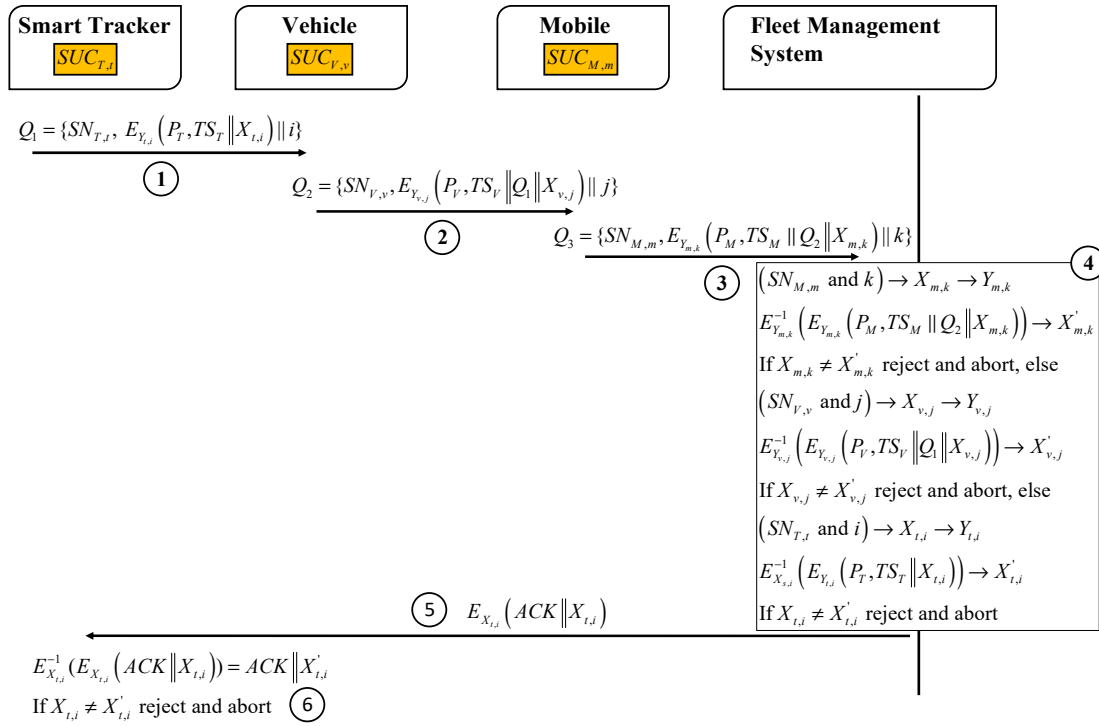


Figure 10. Secure and efficient position tracking protocol.

This protocol can be used also to share other information with FMS such as vehicle events and violations (hard braking, vehicle speed limit, etc.). In some use-cases, there is only two participating fleet management entities with the FMS in the physical chain, such as vehicle and mobile, rather than three FM entities (ST, vehicle, and mobile) in the protocol above.

6. Multi-Realm Operational Capability

Sometimes companies must move FM entities to other globally serving operators/companies. Often, for business deals, the new company should be able to personalize these entities securely, and the home company should not have any access to these entities. Figure 11 describes a hand-over process for a visiting entity having SUC_v , moving from FMS_2 to FMS_1 . FMS_1 requests a valid ticket (X_L/Y_L pair) from FMS_2 to start enrollment for the visiting entity.

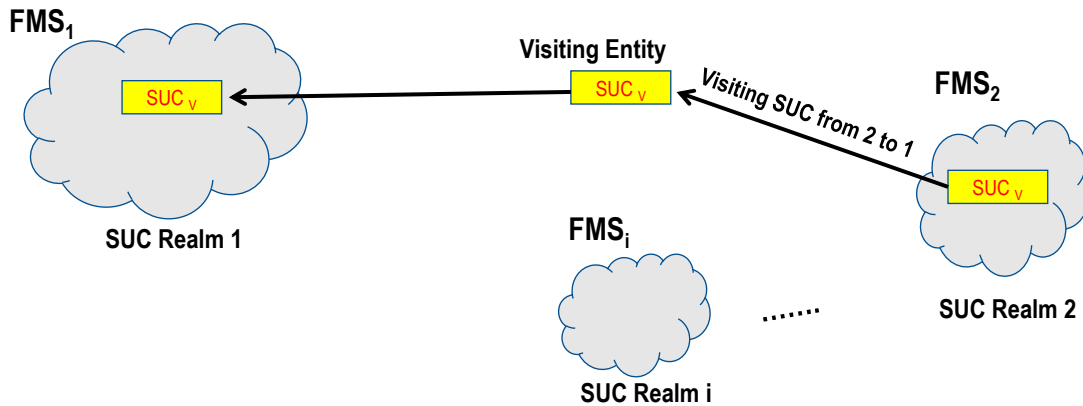


Figure 11. Secured handover process.

Protocol 5: Entity Handover Protocol**Objective**

- Entity Handover: Fleet Manager FMS_1 requests control for a fleet entity from another FMS_2 .

Prerequisites

- FMS_2 agreed to hand over the fleet entity to FMS_1

Output

- FMS_1 enrolls entity successfully

Steps

- FMS_1 requests a ticket for the visiting entity with SUC_v from FMS_2
- FMS_2 sends a valid pair X_L/Y_L as a one-time-ticket to FMS_1 ,
- FMS_1 uses the ticket to enroll entity v , having SUC_v , by sending a set of challenges and receiving the corresponding set of responses from entity v . Then, it stores the CRPs in the FMS backend UIR table.

Figure 12 describes a hand-over protocol (Protocol 5).

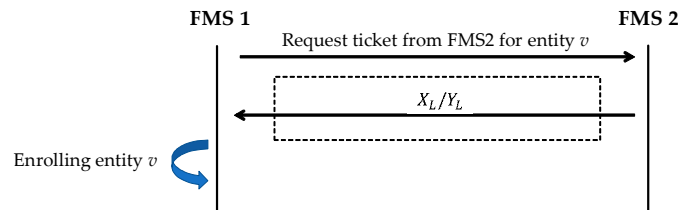


Figure 12. Entity handover protocol from FMS_2 to FMS_1 .

7. Security Analysis

In order to analyze the proposed authentication protocols, several attack scenarios are postulated, such as replay and impersonation attacks. However, an attacker may intercept the message between nodes A and B . Thereupon, the attacker cannot decrypt the transmitted messages without having SUC. Therefore, attacks on SUC and on protocols will be discussed in the following.

7.1. Cloning Complexity of FM Entities

To impersonate an FM entity, an adversary could try to reverse or clone the targeted FM entity. In our proposed security architecture, each FM entity embeds an SUC as a digital clone-resistant and unique function. An intruder aiming to impersonate an FM entity should clone its SUC. There are two types of possible cloning attack on SUCs: mathematical cloning and physical cloning.

- Mathematical cloning:** SUCs are designed so that they are resistant against known mathematical attacks, such as in [27–29]. The attacks' complexity on SUCs is greater than 2^{80} which fulfills today's security limits.
- Physical cloning:** An adversary with physical access to FM entities could try to reverse the embedded SUCs by means of side channel attacks. It was shown, for instance in [28] that such an attack is infeasible since applying SCA requires knowledge of the SUC design structure with its mappings which are unknown to anybody.

We conclude that such attacks are infeasible on the proposed FMS.

7.2. Impersonation Attack on FM Entities

In the presented security protocols, the shared queries between two FM entities of an FM entity and the FM backend system have the form of: $E_X(Data||X)||Y$ Where X/Y denotes the challenge/response pair of an FM entity.

To impersonate the targeted entity having SUC, an adversary should be able to reverse the corresponding X of Y . Since cloning SUC is infeasible (as described in the previous attack), an adversary should reverse the cipher E . E is a standard cipher such as AES and hence it is infeasible to apply such an attack. An invasive physical replacement attack was analyzed in previous work [35].

7.3. Location Tracking Attacks on FMS

In this attack, an adversary tries to get positions information about FM entities. In the proposed protocols in this work, FM entities positions can be shared with the FMS in Protocols 2, 3, and 4. Notice that in these protocols, all shared queries and responses are encrypted by using a standard cipher E keyed with X , which denotes an FM entity's SUC^{-1} response to a challenge Y . This type of adversary has two possible scenarios to get an FM entity position information: breaking the standard cipher E , which is assumed to be secure against known mathematical attacks, or the adversary could try to recover X from Y and then be able to decrypt the captured shared message between an FM entity and the FMS. The last attack requires breaking the deployed SUC, which is designed to be secure against mathematical and physical attacks. Hence, the proposed protocol in this work are secure against this type of attacks.

7.4. Eavesdropping Attacks on FMS Communication Links

Eavesdropping attack is known also as sniffing or snooping attack. In this attack, an adversary captures the network traffic between FM entities or an FM entity and the FMS backend system, then the adversary tries to gain information from the captured messages. Notice that all the network traffic in the proposed security architecture is encrypted by using a standard cipher keyed with X , which denotes an FM entity's SUC^{-1} response to a challenge Y . As shown also in the previous attack, gaining information from these encrypted packets is not possible because of the high attack complexity to break either the standard cipher E or an SUC (attack complexity greater than 2^{80}).

7.5. Replay Attack

In the replay attack, the adversary somehow collects signals from a device to re-send and reuse. The target of the adversary is fooling the legitimate devices that have completed the protocol run. Randomly selecting a value X from the list of pairs makes a replay attack difficult and the SUC's one-time use pairs increase the security level of the FMS to be completely secure against a replay attack.

8. Conclusions

A novel security architecture mapped onto future Fleet Management System (FMS) is proposed. The new architecture is based on embedding digital SUCs in all FMS-security-relevant components such as vehicles, goods and mobiles to make them clone-resistant or unclonable. SUCs as clone-resistant identities can be embedded in all security relevant units in a "post-fabrication process" by the FMS-trusted-authority (TA) to keep device manufacturers out of the security process when necessary. This is often a fundamental requirement when low-cost "un-trustable" mass-production-manufacturers are involved. The proposed SUC structures as invertible ciphers, offer very efficient management of provable identities compared with the traditional PUF technology. The resulting system would make any physical replacement attacks on any security-relevant FMS entity very hard or impossible. Sample generic SUC-based protocols are presented to demonstrate how to protect the FMS against many types of attacks. The system is shown to be highly flexible (multi-realm capable), scalable, and extendable to cover virtually all severe attack scenarios. The proposed FMS security requirements are expected to become a "must-have" requirement in the future FMSs operating at open network with globalized smart vehicular infrastructure. The proposed digital clone-resistant SUC technique is highly resilient. It has no aging issues compared to traditional analog PUF technology, which tends to be very costly, inconsistent, and highly complex to manage. The involved SUC authentication protocols are much simpler and highly efficient and manageable when compared to the traditional

PUF techniques, which are equivalent to unknown non-invertible hash functions. Finally, there is a crying need for highly secured FMSs and automated trustable goods exchange at low-cost and on secured basis. This would remarkably contribute to improve fair exchange of goods between nations and possibly leads to more peace and less international goods-exchange- criminalities in general.

Author Contributions: Conceptualization, E.H.; methodology, E.H., A.M. and W.A.; validation, E.H., A.M. and W.A.; formal analysis, E.H. and A.M.; investigation, E.H. and A.M.; resources, W.A.; writing—original draft preparation, E.H. and A.M.; writing—review and editing, E.H., A.M. and W.A.; visualization, E.H. and A.M.; supervision, W.A.; project administration, W.A.; funding acquisition, W.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Volkswagen AG and Microsemi, a Microchip Company, San Jose USA as well as the German Federal Foreign Office funding by DAAD combined scholarship and support program (STIBET).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. IRP & IFTA (Apportioned Plates & Fuel License). Available online: <http://interstateauthority.com/irp.aspx> (accessed on 31 October 2019).
2. Kishore, T.K.; Vardhan, T.S.; Narayana, N.L. Vehicle Tracking Using a Reliable Embedded Data Acquisition System with GPS and GSM. *Int. J. Comput. Sci. Netw. Secur.* **2010**, *10*, 286–291.
3. Hsiao, M.; Chang, S.K.J. The optimal location update strategy of cellular network based traffic information system. In Proceedings of the 2006 IEEE Intelligent Transportation Systems Conference, Toronto, ON, Canada, 17–20 September 2006; pp. 248–253.
4. Fan, X.B.; Xu, W.; Chen, H.; Liu, L. CCSMOMS: A composite communication scheme for mobile object management system. In Proceedings of the 20th International Conference on Advanced Information Networking and Applications—AINA’06, Vienna, Austria, 18–20 April 2006; Volume 1, pp. 235–239.
5. US Fleet Tracking—GPS Tracking, Devices, and Service. Available online: <https://www.usfleettracking.com/> (accessed on 29 April 2019).
6. RoadLog ELD Plus with wireless Connectivity|VDO RoadLog™. Available online: <https://www.vdoroadlog.com/electronic-logging-devices-eld/roadlog-eld-plus/> (accessed on 29 April 2019).
7. Stübing, H.; Bechler, M.; Heussner, D.; May, T.; Radusch, I.; Rechner, H.; Vogel, P. simTD: A car-to-X system architecture for field operational tests [Topics in Automotive Networking]. *IEEE Commun. Mag.* **2010**, *48*, 148–154. [CrossRef]
8. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153. [CrossRef]
9. The Gold Nuggets in the Supply Chain: A Tracker That Makes Shipping Pallets Smart—Deutsche Telekom. Available online: <https://www.telekom.com/en/media/media-information/archive/telekoms-tracker-makes-shipping-pallets-smart-547120> (accessed on 30 April 2019).
10. Peer, P.; Bule, J.; Gros, J.Z.; Štruc, V. Building cloud-based biometric services. *Informatica* **2013**, *37*, 115–122.
11. Xu, G.; Li, M.; Luo, L.; Chen, C.H.; Huang, G.Q. Cloud-based fleet management for prefabrication transportation. *Enterp. Inf. Syst.* **2019**, *13*, 87–106. [CrossRef]
12. Giacobbe, M.; Puliafito, A.; Villari, M. A service oriented system for fleet management and traffic monitoring. In Proceedings of the IEEE Symposium on Computers and Communications, Riccione, Italy, 22–25 June 2010; pp. 784–786.
13. Billhardt, H.; Fernández, A.; Lemus, L.; Lujak, M.; Osman, N.; Ossowski, S.; Sierra, C. Dynamic coordination in fleet management systems: Toward smart cyber fleets. *IEEE Intell. Syst.* **2014**, *29*, 70–76. [CrossRef]
14. Gowda, V.R.C.; Gopalakrishna, K. Real time vehicle fleet management and security system. In Proceedings of the 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, India, 10–12 December 2015; pp. 417–421.
15. Malekian, R.; Moloisane, N.R.; Nair, L.; Maharaj, B.T.; Chude-Okonkwo, U.A.K. Design and Implementation of a Wireless OBD II Fleet Management System. *IEEE Sens. J.* **2017**, *17*, 1154–1164. [CrossRef]

16. Aloquili, O.; Elbanna, A.; Al-Azizi, A. Automatic vehicle location tracking system based on GIS environment. *IET Softw.* **2009**, *3*, 255. [\[CrossRef\]](#)
17. Stojanovic, D.; Papadopoulos, A.N.; Predic, B.; Djordjevic-Kajan, S.; Nanopoulos, A. Continuous range monitoring of mobile objects in road networks. *Data Knowl. Eng.* **2007**, *64*, 77–100. [\[CrossRef\]](#)
18. Civilis, A.; Jensen, C.S.; Pakalnis, S. Techniques for efficient road-network-based tracking of moving objects. *IEEE Trans. Knowl. Data Eng.* **2005**, *17*, 698–712. [\[CrossRef\]](#)
19. Raya, M.; Hubaux, J.-P. The security of VANETs. In Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks—VANET '05, Cologne, Germany, 2 September 2005; ACM Press: New York, NA, USA, 2005; pp. 93–94.
20. Choudhary, S.; Purohit, K. VANET: Its applications, security requirements, types of attacks and its corrective measures. In Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 28–29 September 2018; pp. 883–888.
21. Ravikanth, P.S. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030.
22. Lofstrom, K.; Daasch, W.R.; Taylor, D. IC identification circuit using device mismatch. In Proceedings of the 2000 IEEE International Solid-State Circuits Conference, Digest of Technical Papers (Cat. No. 00CH37056), San Francisco, CA, USA, 9 February 2000.
23. Gassend, B.; Clarke, D.; van Dijk, M.; Devadas, S. Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security—CCS '02, New York, NY, USA, November 2002; pp. 148–160. Available online: <https://dl.acm.org/citation.cfm?id=586132> (accessed on 31 October 2019).
24. Bösch, C.; Guajardo, J.; Sadeghi, A.-R.; Shokrollahi, J.; Tuyls, P. Efficient helper data key extractor on FPGAs. In Proceedings of the 10th International Workshop on Cryptographic Hardware and Embedded Systems, Washington, DC, USA, 10–13 August 2008; pp. 181–197.
25. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology—EUROCRYPT 2004*; Cachin, C., Camenisch, J.L., Eds.; Springer: Berlin, Germany, 2004; Volume 3027, pp. 523–540.
26. Adi, W.; Mars, A.; Mulhem, S. Generic identification protocols by deploying secret unknown ciphers (SUCs). In Proceedings of the 2017 IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW), Taipei, Taiwan, 12–14 June 2017.
27. Mars, A.; Adi, W. Digitally Mutating NV-FPGAs into Physically Clone-Resistant Units. *arXiv* **2019**, arXiv:1908.03898. Available online: <https://arxiv.org/ftp/arxiv/papers/1908/1908.03898.pdf> (accessed on 31 October 2019).
28. Mars, A.; Adi, W. New Family of Stream Ciphers as Physically Clone-Resistant VLSI-Structures. *Cryptography* **2019**, *3*, 11. [\[CrossRef\]](#)
29. Mars, A.; Adi, W.; Mulhem, S.; Hamadaqa, E. Random stream cipher as a PUF-like identity in FPGA environment. In Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 209–214.
30. Mars, A.; Adi, W. Clone-Resistant Entities for Vehicular Security. In Proceedings of the IEEE 13th International Conference on Innovations in Information Technology (IIT), Al Ain, UAE, 18–19 November 2018; IEEE: Piscataway, NJ, USA, 2018.
31. Mastali, N.; Agbinya, J.I. Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper. In Proceedings of the 2010 Fifth International Conference on Broadband and Biomedical Communications, Malaga, Spain, 15–17 December 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–6.
32. Peralta, D.; Galar, M.; Triguero, I.; Paternain, D.; García, S.; Barrenechea, E.; Benítez, J.M.; Bustince, H.; Herrera, F. A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Inf. Sci.* **2015**, *315*, 67–87. [\[CrossRef\]](#)
33. Limbasiya, T.; Doshi, N. An analytical study of biometric based remote user authentication schemes using smart cards. *Comput. Electr. Eng.* **2017**, *59*, 305–321. [\[CrossRef\]](#)

34. Bhagavatula, C.; Ur, B.; Iacovino, K.; Kywe, S.M.; Cranor, L.F.; Savvides, M. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In Proceedings of the 2015 Workshop on Usable Security, San Diego, CA, USA, 8 February 2015; Internet Society: Reston, VA, USA, 2015.
35. Hamadaqa, E.; Mulhem, S.; Mars, A.; Adi, W. Clone-Resistant Joint-Identity Technique for Securing Fleet Management Systems. In Proceedings of the 2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Edinburgh, UK, 6–9 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 327–332.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).