Fortifying Connected Vehicles Based Cybersecurity Measures for Secure Over-the-Air Software Updates

Shashikant Patil[1*], Senthil Kumar A.[2], Saket Mishra[3], N. Gobi[4], Intekhab Alam[5], Romil Jain[6]
[1]Professor, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India
[2]Professor, Computer Science and engineering, School of engineering, Dayananda Sagar University, Bangalore, India
[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India
[4]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India
[5]Assistant Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[6]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India
Emails: shashikant.patil@atlasuniversity.edu.in; angusen@gmail.com; saket.mishra.orp@chitkara.edu.in; gobi.n@jainuniversity.ac.in; intekhab@muit.in; romil.jain.orp@chitkara.edu.in

Abstract

The emergence of connected vehicles has transformed the automotive sector by enhancing the vehicle's functionality, efficiency, and safety. The performance and security of these vehicles significantly rely on the deployment of the over-the-air software update. However, the execution of OTA comes with many challenges, especially with regard to security vulnerabilities and risks. The current paper delves into the complexities of the secure OTA software update for connected vehicles addressing the most critical issues; authentication; encryption and integrity verification, and risk management. Through advanced cryptographic methodologies, stringent authentication processes, and secure communication channels, automotive manufacturers and other service providers can guarantee the integrity and confidentiality of the updates, and consumers' data from malicious attack. Moreover, the paper explores the regulatory and other standards-related matters that control the use of OTA in the automotive sector. An understanding of the secure OTA update mechanisms aids the stakeholders in establishing a resilient connection in connected vehicles boosting consumer trust and the future of the automobiles industry.

Keywords: Connected vehicles; Over-the-air updates; Security; Authentication; Encryption; Integrity verification; Risk mitigation; Regulatory compliance

1. Introduction:

Over the years, updating a vehicle's software [1] has been exponentially time-consuming because it required physical intervention, such as visits to the dealership. [2] Today, the process seems less cumbersome and more user-friendly due to the technology available in this sphere . Therefore, the modern vehicle is updated not physically, but firmware transmitted over the air using wireless communication links. [3].

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

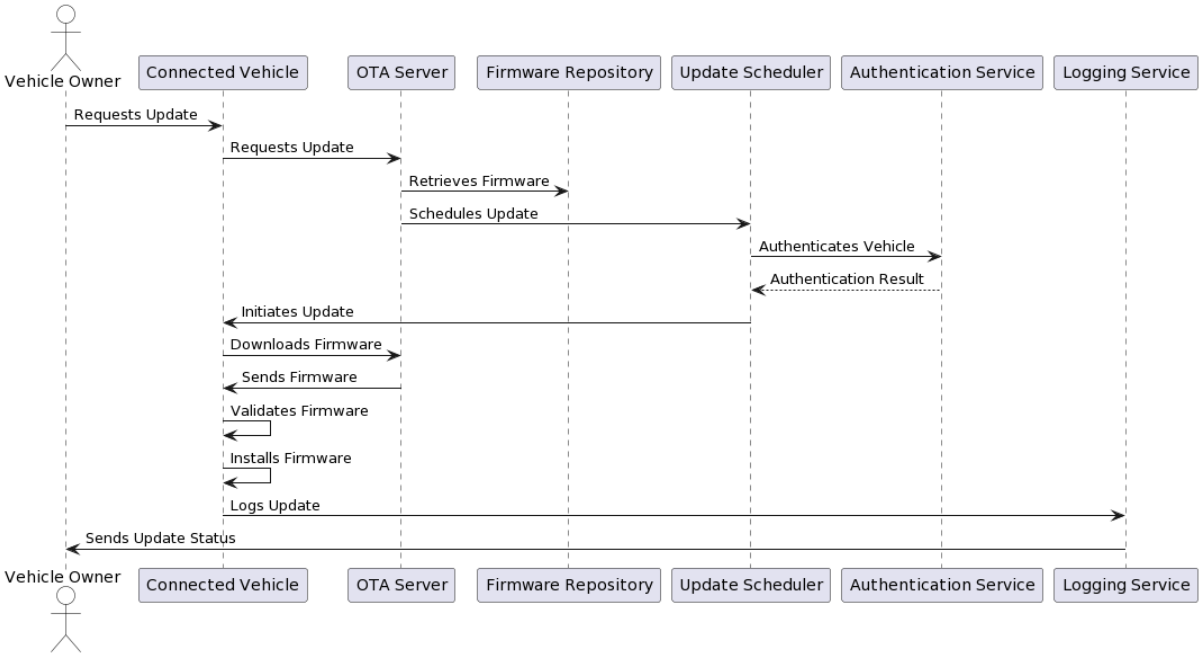

Figure 1: Over-the-Air (OTA) updates in Autonomous Vehicles

According to Figure 1, the reasons for OTA updates implementation in the automotive field include the following factors. Due to the growing complexity of vehicle software such as infotainment systems and advanced driver-assistance systems , the car developers are faced with a broad spectrum of vehicle software enablement for different functionalities. Cars become susceptible and responsive to the software applications and computer-operated components. Such a challenge becomes vital in terms of intensive response to the system bugs, vulnerabilities, performance issues, etc. to ensure the optimal performance and maintain safety.

1.1 Evolution of Connected Vehicles

The history of connected vehicles represents a transformative trajectory in the automotive industry driven by technological advancements and changing consumer preferences Sixth. The trajectory of the evolution includes the following stages. In the late 20th century and the early 21st century, telematics systems were emerging, providing vehicles with limited connectivity, such as GPS-based navigation and wireless connections to a service center for emergency help and assistance Seventh. These systems utilized cellular networks and the vehicle's onboard computer. However, the functionality was not available for occupants of the vehicle. The second stage followed with the integration of infotainment. Many consumer electronics products provided extensive connectivity and digital services to their users. Hence, automotive manufacturers started prioritizing such functionality in vehicles as well. Infotainment systems empowered vehicle occupants with numerous digital services and was transformed by time into a media hub accessible to all passengers in the vehicle. The third stage involved the introduction of connected services. Smartphone usage became widespread, and mobile data networks were also expanding. Automotive companies started offering their customers connected services proxied through their smartphones, including real-time monitoring of vehicle status, condition notification, and so forth Eighth. The fourth stage is characterized by the emergence of V2X vehicle communication. V2V, vehicle-to-vehicle, and V2I, vehicle-to-infrastructure, communication are technologies that provide significant safety and efficiency benefits to road traffic. The fifth stage refers to further development of advanced driver-assistance systems, where vehicles get another level of connectivity that significantly reduced the possibility of human errors Ninth. Finally, the transition to CAV connects all the presented concepts. CAV is a connected vehicle modified with artificial intelligence, data mining based on exceptional connectivity, comprehensive onboard sensory systems, and high-tech illustration and navigation. More automobile-oriented applications and their effects are presented.

1.2 Significance of Over-the-Air Software Updates

Over-the-air software updates are groundbreaking for the automotive industry, marking a radical departure from how vehicles are maintained, updated, and enhanced. Conventional methods of software updates have always required physical access to the vehicle, whereas OTA updates allow manufacturers to push remote updates directly to the car

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

through a wireless network. This offers numerous potential benefits that are becoming increasingly necessary as the automotive industry evolves:

High on the list of advantages is that OTA updates increase the efficiency and convenience of software maintenance on the vehicle. Instead of having to visit a dealership or service center to receive vehicle updates, car owners may download them at their leisure without stopping their work routines. This ensures that the vehicle owner will not be inconvenienced by the update process, while the manufacturer will benefit from reduced upgrade costs and customer service demands due to the lack of logistical difficulties .

Second, OTA updates also facilitate manufacturers' ability to react to new issues, vulnerabilities, and cybersecurity risks with tremendous agility.

Lastly, OTA updates make it easier to expand vehicles' lifecycle and functionality over time. As driver preferences and regulations change, producers can adapt to them by uploading updates as new vehicle owners purchase their cars. However, there are a few provisions that must be addressed—especially with regard to security and privacy. In particular, the remote nature of OTA updates creates the following potential concerns, among others: unauthorized access, data breaches, and sabotage of vehicle software through manipulation. The cyber resilience of all OTA authorities should be strengthened to ensure the confidentiality, integrity, and availability of update activities.

1.3 Challenges and Security Concerns

Moreover, OTA updates provide significant improvements in terms of efficiency and cost-effectiveness. For manufacturers, this entails the possibility of carrying out updates remotely, speeding up the deployment time, minimizing downtime, and inconvenience for car owners [15]. This feature leads to increased customer satisfaction and also results in savings through the elimination of manual labor and logistics costs that are necessary when applying updates in traditional ways. Furthermore, OTA updates allow carmakers to offer new functional options to car owners even after its delivery. Whether it be a new type of entertainment, vehicle performance improvements, or an update for avoiding new cyber threats, manufacturers can adapt their product offers to consumer preferences this way. Still, the new approach to applying updates also poses several challenges and risks in terms of security and privacy. The applied mechanism allowing to carry out OTA updates remotely significantly increased the risks of unauthorized access, data leaks, and malicious interference that can disrupt vehicle functionality. Precautionary measures ensuring that the OTA update process is integrable, authentic, and confidential are required in order to ensure the safety and privacy of the vehicle and its owner's data [16]. Contextually, this paper explores the essence of the secure OTA updates for connected cars, reviews the required technology, identifies the security threats, and frameworks, and presents existing best practices in the industry. By raising awareness about implementing secure OTA update mechanisms, it helps integrate future driving ecosystems based on trust and reliability [17] .

Objective of Proposed Work:

The objective of the proposed work is to develop and deploy a comprehensive framework for secure over-the-air software updates for connected vehicles. The proposed framework must adequately address the challenges and risks associated with OTA updates and ensure the integrity, confidentiality, and availability or reliability of vehicle software and be legally compliant. 1) Designing assurance authentication protocols: Produce safe safeguards that can verify the integrity and authenticity of the update source and source authorization. 2) Implementing secure channels: Create secure transmission, shopping, and monitoring stations using encryption measures. 3) Ensuring interoperability: Prove that you accept and protect OTA certification through encryption and transmission regarding the install update packages. 4) Threat intelligence assurance. Define and mitigate cybersecurity risks, including supplier risks, unrealized hacking, or leaks. 5) Regulatory compliance: Meet the certain expectations of regulatory and policy expectations. 8) Improving stakeholders' stakeholder commitment. A method that is used to form the contribution at section 2, potential hazards shared at section 3, and legislative overview are shared at section 4. Case research and evidence-based knowledge framework review are at section 5. A suggested future work and summary is in section 6.

2. Security Foundations for OTA Updates

The block diagram above is a Security Foundations for OTA (Over-the-Air) Update, which is a graphical representation of the aforementioned foundational aspects and their interactions. OTA update systems for connected devices rely on these components to ensure the security of their updates. The diagram illustrates that the Security Protocols are at the heart of the OTA Update System since they include measures that guarantee the confidentiality, authenticity, and integrity of OTA update packages when they are transmitted over the air. Key Management is the final piece of Security Foundations for OTA Update, which is in charge of the encryption, authentication keys and

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

other security mechanisms. It ensures the secure generation, distribution, transmission, and storage of symmetric and asymmetric keys. Table 1 summarizes the components and their explanations. It is represented as a block.

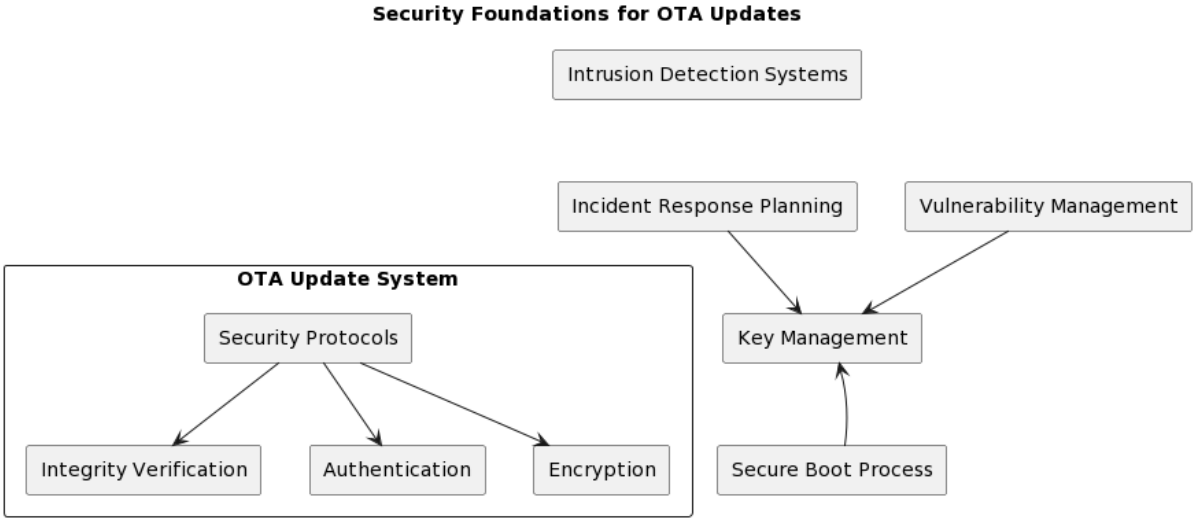

Figure 2: Security foundation of OTA updates

According to Figure 2, Vulnerability Management is critical to scanning regularly and assessing vulnerabilities and fixing them in OTA update systems to identify security flaws and fix them. This ultimately leads to organizations' ability to prioritize flaws and address them with a security fix to improve your overall security posture . Finally, Incident Response Planning helps organizations address security incidents and violations affecting OTA software updates. This involves developing a detailed and actionable incident management plan with procedures, officers, and response teams to quickly and effectively handle violations that occur.

2.1 Authentication Mechanisms

Authentication mechanisms are essential in determining the identity of the entities involved in the OTA update. Specifically, one of the popular authentication techniques is based on digital signatures, which, in turn, are described in the context of asymmetric cryptography . In this process, the signature authority creates a singular pair of cryptographic keys during the signature issuing – the public key intended for the sign issuer and its urge secret-kept private key. The signature authority signs the OTA update using a private key generating a digital signature checked easily by all its possessors who possess the related public key . Mathematically, the signature issuing and verifying comply with the next relation:

$$\sigma = m^d \bmod n$$
$$m = \sigma^e \bmod n \quad (1)$$

Where:

- σ is the digital signature,
- m is the message,
- d is the private key,
- e is the public key, and
- n is the modulus.

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

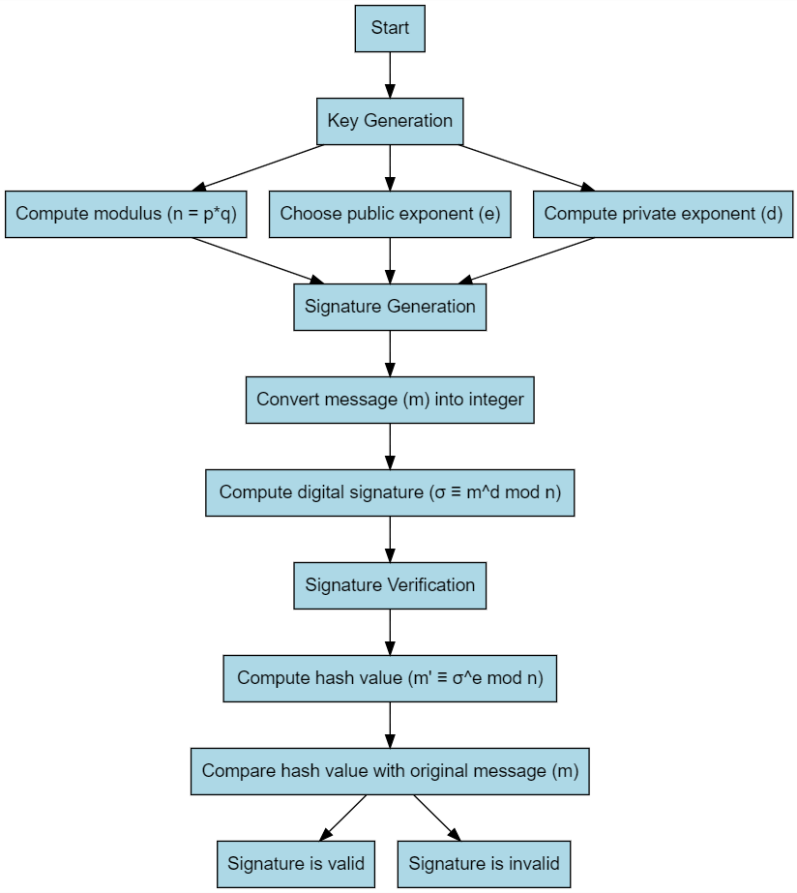

Figure 3: RSA Signature Generation and Authentication process

RSA Signature Generation:

The process of generating a digital signature (σ) for a message (m) using RSA involves the following steps:

1 Key Generation:

Generate two large prime numbers, p and q. Compute the modulus, $n = p^{*}q$. Choose an integer e (public exponent) such that $1 < e < \varphi(n)$ and

$$\gcd(e, \varphi(n)) = 1 \quad (2)$$

where $\varphi(n)$ is Euler's totient function.

$$d^{*}e \equiv 1(\mathrm{mod}\varphi(n)). \quad (3)$$

Signature Generation:

$$(d): \sigma \equiv m\text{^}d(\mathrm{mod}n). \quad (4)$$

RSA Signature Verification:

$$m' \equiv \sigma^{e}\mathrm{mod}n \quad (5)$$

$$m' \equiv \sigma^{e}\mathrm{mod}n \quad (6)$$

Where:

- m' is the computed hash value,
- σ is the digital signature,
- e is the public key exponent, and
- n is the modulus.

2.2 Encryption Techniques

The most important concept to consider in terms of guaranteeing the confidentiality of data transmitted during an OTA update is encryption techniques. The Advanced Encryption Standard employed commonly for encryption is a symmetric-key cipher [20] that is usually referred to as AES . AES performs its operations on fixed-sized blocks of

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

data containing 128 bits, plus it supports key lengths of 128,192, or 256 bits. The encryption is done by repeating a sequence of rounds that consist of substitution, permutation, and mixing functions. The mathematical description of AES encryption is below:

$$C = \text{AES}_K\ (P) \tag{7}$$

Where:

- C is the ciphertext,
- AES_K is the AES encryption function with key K, and
- P is the plaintext.

1 SubBytes:

$$\text{SubBytes}\ (S) = \begin{bmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{bmatrix} \rightarrow \begin{bmatrix} \text{SBox}\ [s_0] & \text{SBox}[s_1] & \text{SBox}[s_2] & \text{SBox}[s_3] \\ \text{SBox}[s_4] & \text{SBox}[s_5] & \text{SBox}[s_6] & \text{SBox}[s_7] \\ \text{SBox}[s_8] & \text{SBox}[s_9] & \text{SBox}[s_{10}] & \text{SBox}[s_{11}] \\ \text{SBox}[s_{12}] & \text{SBox}[s_{13}] & \text{SBox}[s_{14}] & \text{SBox}[s_{15}] \end{bmatrix} \tag{8}$$

2 ShiftRows:

$$\text{ShiftRows}\ (S) = \begin{bmatrix} s_0 & s_5 & s_{10} & s_{15} \\ s_4 & s_9 & s_{14} & s_3 \\ s_8 & s_{13} & s_2 & s_7 \\ s_{12} & s_1 & s_6 & s_{11} \end{bmatrix} \tag{9}$$

3 MixColumns:

$$\text{MixColumns}\ (S) = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{bmatrix} \tag{10}$$

4 AddRoundKey:

$$\text{AddRoundKey}\ (S, K) = S \oplus K \tag{11}$$

Where:

- S is the state matrix,
- K is the round key, and
- $\oplus$ denotes the bitwise XOR operation.

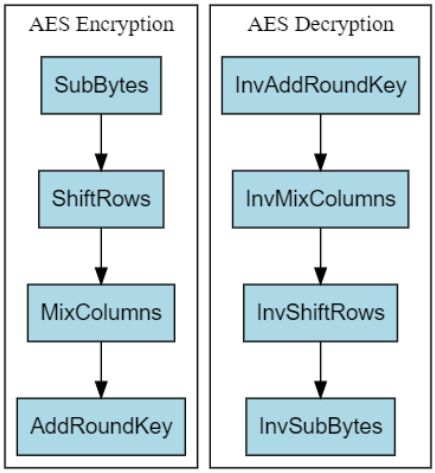

Figure 4: Authentication using AES Encryption and Decryption

By referring to Figure 4, OTA updates for connected vehicles can safely transmit through wireless networks through AES encryption while honoring the confidentiality and integrity of the update packages. AES is especially known for its robustness and efficiency and has proven a common choice for securing sensitive data in several applications, including automotive systems . Using AES encryption, manufacturers can protect OTA updates from any form of

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

cyber-attack, such as eavesdropping, tampering, and so forth, to heighten the security level of connected cars and to protect against any imminent threats in the digital world.

2.3 Integrity Verification

Integrity verification mechanisms are essential for detecting any unauthorized modifications or tampering with OTA update packages. One commonly employed technique is the use of cryptographic hash functions, such as SHA-256 as shown in Figure 5.

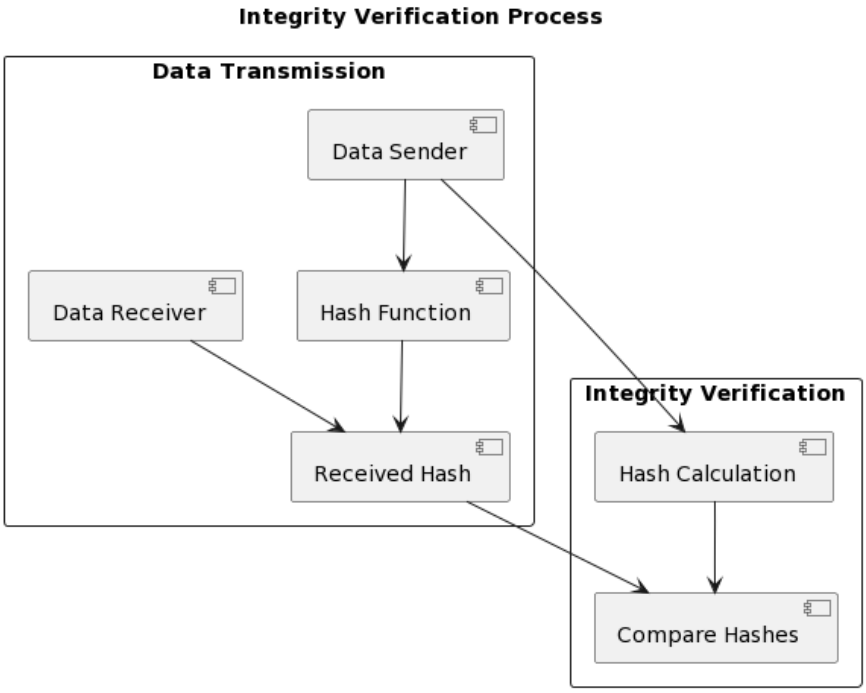

Figure 5: Integrity verification process working model

The hash function generates a fixed-size digest (hash value) based on the input data, which uniquely represents the content of the OTA update package. Mathematically, the integrity verification process involves computing the hash value (H) of the OTA update package (P) and comparing it with the expected hash value (H′) :

$H = \text{SHA} - 256(P)$ (12)

$H' =$ Expected Hash Value

2.4 Secure Boot Process:

The secure boot process is crucial for ensuring the integrity and authenticity of the firmware or software image loaded during the boot sequence.

One common approach is to use a secure boot loader that verifies the digital signature of the firmware image before executing it. Mathematically, the secure boot process involves verifying the digital signature (σ) of the firmware image (F) using the public key (e) stored in the device's trusted boot firmware:

$F = \sigma^e \text{mod} n$ (13)

Where:

- F is the firmware image,
- σ is the digital signature,
- e is the public key, and
- n is the modulus.

Secure boot is a necessary process for verifying the integrity and authenticity of firmware or software that is loaded during the boot of a device. It is a measure used in web security and connected vehicles among other technological setups. It is used to ascertain that the firmware or any reasonable code has been properly and signed before execution to prevent unauthorized and malicious code from running. The boot is implemented in several steps as outlined below. The secure boot process is initiated after the device is powered on or reset. The boot firmware, usually known as the bootloader, starts the boot process by booting the next firmware stage or the operating system kernel. The bootloader uses a trusted public key to verify the digital signature of the firmware or software image. The public key is secured

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

in the device, either a secure element or a trusted processor module at the device. The bootloader then takes a ahs and compares it with the image's public key hash. If the images' hashing matches the hash, then the image has not been compromised since it has been signed.

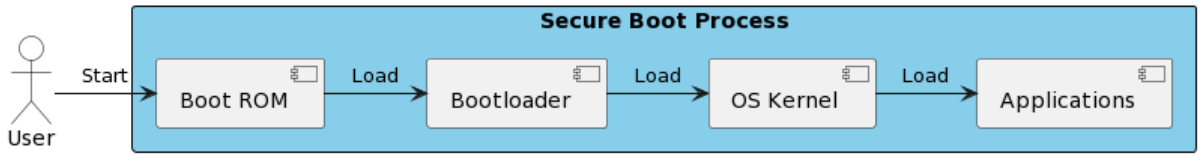

Figure 6: Secure Boot Process

The secure boot process in Figure 6 establishes a chain of trust that ensures that each subsequent stage of the boot firmware or the software image is verified before execution. This chain of trust extends from the bootloader into the boot firmware and the OS kernel and into any other software image that loads during the boot process. The secure boot process will then allow the bootloader to execute the firmware or software image if it were successfully verified . This feature of the secure boot process ensures that the only validated, authenticated code is allowed to run on the device hence, preventing unauthorized access and malicious cyber-attacks. In the instance that the verification check for the firmware or software image file fails, the secure boot process halts the boot sequence or initializes a recovery mechanism; thus, it does not execute the potentially compromised code to ensure the device maintains its security posture. In summation, the secure boot process is a vital security feature that protects connected vehicles and other devices from unauthorized access attacks. The secure boot process verifies the validity and integrity of the software image and firmware; thereby, enhancing the datatype of the boot firmware to protect the whole datatype

3. Risk Mitigation Strategies

In Risk Mitigation intrusion detection systems, vulnerability management, and incident response planning in the context of securing over-the-air (OTA) software updates for connected vehicles.

3.1 Threat Modelling

Threat modeling is a method that systematically identifies and prioritizes potential threats to a system's or application's security. When it comes to OTA software updates for connected cars, a threat model determines the attack vectors, vulnerabilities, and malicious scenario that can be exploited by attackers against a solution. The STRIDE model is a common method for modeling which consists of 6 categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege . Mathematically, threat modeling is a matter of assessing the likelihood and impact of the risks L, and I, which can be expressed in the risk score in formula :

$$R = L \times I \quad (14)$$

By quantifying the risks associated with different threats, organizations can prioritize mitigation efforts and allocate resources effectively to enhance the security of OTA updates for connected vehicles.

3.2 Intrusion Detection Systems:

Intrusion Detection Systems (IDS) play a crucial role in detecting and alerting organizations to potential security breaches or unauthorized access attempts. IDS can be deployed at various points within the OTA update ecosystem, including network gateways, end point devices, and backend servers.

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

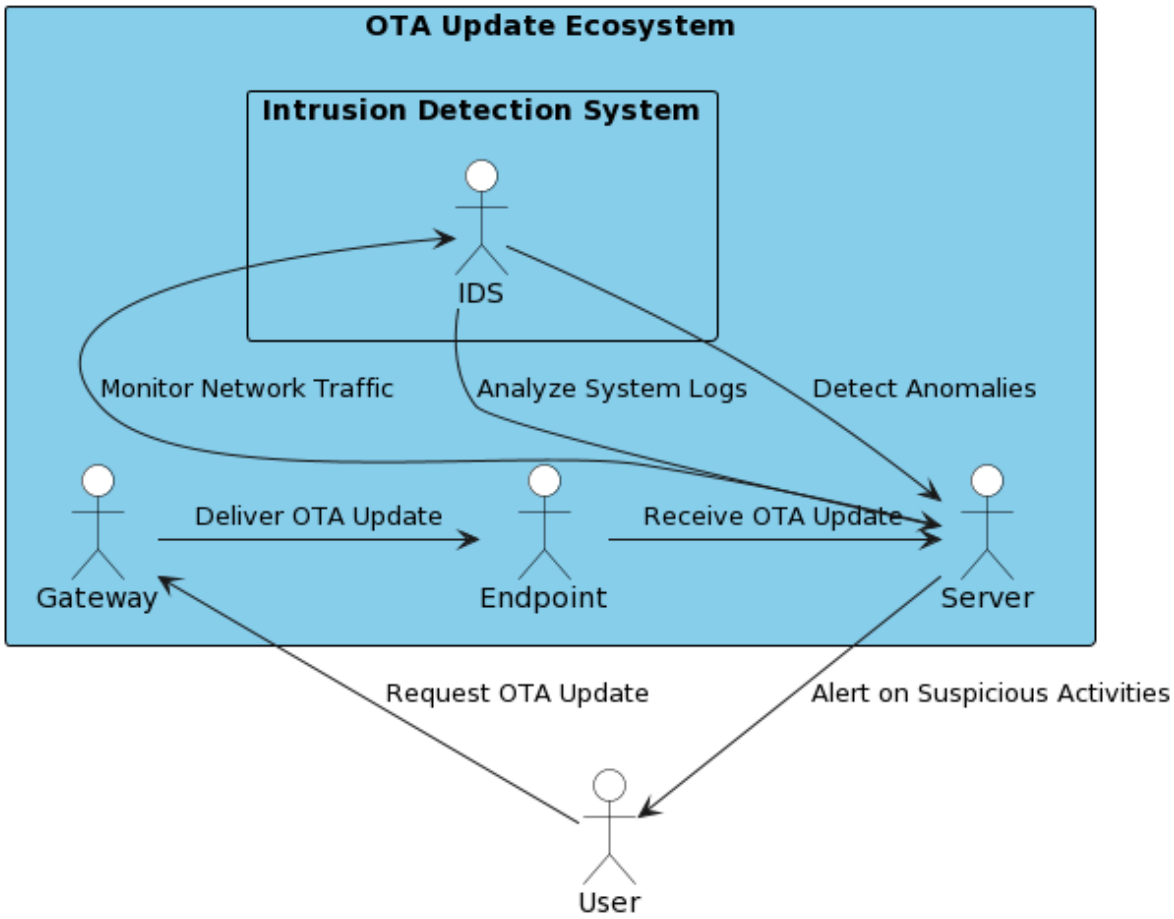

Figure 7: OTA update flowchart with user activities

From Figure 7 , IDS analyze network traffic patterns, system logs, and other indicators of compromise (loC) to identify suspicious activities. One common approach used in IDS is anomaly detection, where deviations from normal behavior are flagged as potential security incidents.

3.3 Vulnerability Management:

Vulnerability Management – is a proactive approach used to identify, assess, and mitigate vulnerabilities in software and systems. In the context of OTA updates or connected vehicles, vulnerability management is constantly scanning the OTA update infrastructure for security vulnerabilities that include software components, network protocols, and communication channels. The mathematics behind vulnerability management involve the calculation of Vulnerability Score , based on the severity and exploitability of a with the following equation :

$$VS = S \times E \quad (15)$$

where Severity is the severity of the vulnerability, usually scored from 1 to 10, and Exploitability is the likelihood of the vulnerability being exploited. By ensuring that actions are taken with respect to the vulnerability score as achievable in the mitigation factors, an organization can minimize risks and make OTA updates for connected vehicles safer.

3.4 Incident Response Planning:

Regarding incident response planning, it creates a comprehensive set of procedures and protocols for taking action during security incidents and breaches. For the connected vehicle OTA, this will imply creating a dedicated incident response team, delineating roles and responsibilities, and establishing an incident response plan . The formula, where incident response planning is calculated mathematically, is Mean Time To Detect and Mean Time To Response :

$$MTTD = \frac{\text{Total time to detect incidents}}{\text{Number of incidents}} \quad (16)$$

$$MTTR = \frac{\text{Total time to respond to incidents}}{\text{Number of incidents}} \quad (17)$$

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

Organizations can lessen the impact of security incidents and guarantee the discovery and quick reaction to likely threats and issues. In summary, Threat modeling, IDSs, VM, and incident response these approaches have been discussed. Theses all aspects are useful to conducting required securing measures presents a thesis securing and all of the data-driven mathematical models to provide Ota uploads with a secure and reliable and protect the software of the connected vehicle from the functionality indicating to create cars.

4. Regulatory Landscape and Standards

4.1 Legal Frameworks and Compliance Requirements

According to the user, in the realm of secure over-the-air software updates for connected vehicles, case studies and practical implementations are central to providing insights into their real-world use, as well as how effective different strategies are. Some of the case studies and practical implementation summaried include: In addition to the legal requirements, industry standards and best practice can be defined to describe the level of excellence that firms desire to achieve through best practice and such in order to ensure the security, reliability, and interoperability of OTA updates for connected vehicles. The International Organization for Standardization , Society of Automotive Engineers , and Automotive Industry Action Group are examples of organizations that have published standards and guidelines that are tailored to the automotive industry: For example ISO/SAE 21434 frames the automotive cybersecurity engineering and provides the process and requirements of automotive systems to be developed and maintained securely. Equally, SAE J3061 offers an engineering approach for vehicle systems cybersecurity and contains such topics including: Legal frameworks and compliance requirements are also factors in the over-the-air (OTA) software updates that shape the landscape for connected vehicles. Laws and regulations have been established by governments and governing bodies around the world to address the most pressing concerns in safety, data privacy, and consumer protection dealing with connected vehicles. Compliance with these legal frameworks is crucial for automobile manufacturers and service providers need to comply with to maintain trust upon the security and privacy of the OTA updates: For example, in the European Union, the General Data Protection Regulation, or GDPR, includes stringent processing and safeguard requirements for personal information. Automakers and service providers must have the appropriate data protection in place when gathering, processing, and transmitting personal data in ‘Updates’ :

$$\text{Compliance} = \begin{cases} 1 & \text{if compliance requirements are met} \\ 0 & \text{otherwise} \end{cases} \quad (18)$$

By implementing appropriate data protection measures, conducting regular audits, and maintaining documentation of compliance efforts, automotive manufacturers and service providers can demonstrate adherence to legal frameworks and mitigate legal risks associated with OTA updates for connected vehicles.

4.2 Industry Standards and Best Practices

iven the relative novelty of secure over-the-air software updates for connected vehicles, the case studies and practical examples represent one of the best measures to explore the real-world application and feasibility of various strategies. We have outlined summaries of some of the most prominent cases in the previous section. Apart from being required to comply with relevant laws, the industry must follow the standards and best practices that offer crucial directions and benchmarks to meet security, reliability, and compatibility objectives. Generally, the International Organization for Standardization , the Society of Automotive Engineers, and the Automotive Industry Action Group have established standards and guidelines specific to the industry. ISO/SAE 21434 on automotive cybersecurity engineering describes a framework that defines the processes and requirements for developing and maintaining secure automotive systems. Conversely, SAE J3061 on cybersecurity engineering for vehicle systems offers guidance on threat modeling, threat assessment, and security controls . Additionally, industry consortia have been established to promote cooperation between automotive manufacturers, suppliers, and cybersecurity professionals and share the latest threat intelligence and best practices to improve connected vehicle security. A relevant example is the Automotive Information Sharing and Analysis Center

5. Case Studies and Practical Implementation

Case Study 1: Tesla's Continuous OTA Updates

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

Tthe software is automatically deployed across the vast array of Tesla vehicles using over & air (OTA) update technology , a major factor which has already led to numerous enhancements in both performance and functionality while at the same time protecting their products from the threats posed by cyber-attackers . The company was meticulous about updating all their systems at the same time, erasing both bugs and vulnerabilities and adding new functions such as protection against cyber-attacks .The download and installation of updates are accomplished automatically with secure protocols that employ differential updates for efficient bandwidth usage, secure authentication links and encryption .It has also built a rollback feature into its products which will take a car back to where it was before an update made other things unstable, as well as these being stable features.

Case Study 2: BMW's Remote Software Upgrade Platform

BMW has added Remote Software Upgradeing capabilities to enable it to carry out its OTA updates without fractionation of operations using IP connected car technology. With this platform, BMW can deliver updated files without needing any disruption from time to source out the update data again. The platform exists for one reason only - that is, it's available as per certain provisions of BMW customer contracts for the purpose of online services. The platform provides secure communication links like HTTPS and end-to- end encryption both to protect update data from exposure during its transmission BMW particulary prefers to use incremental updating in order to conserve bandwidth. It has also set up certificate-based verification both of the update source and the matching number installed, to assure dependability and prevent tampering. Please see figure Regular safety tests are made for each model of car to find any trouble spots, ensuring that OTA updates are both secure and reliable.

Airbiquity's OTAmatic® OTA Software Management Solution

One such example is OTAmatic® solution from Airbiquity, which provides systems engineers with OTA (over-the-air) software management capabilities. The development itself includes its own FOTA Gateway system for secure data transmission The Fota chapter provides both data confidentiality and data integrity between endpoints, using role-based access control along with a digital signing mechanism that can verify integrity. For products wherever deployment situation or device configuration varies from the norm, OTAmatic offers the flexibility and multi-level process you need.

Continental's OTA Connect® Solution

OTA Connect® by Continental is a software platform that provides advanced over-the-air update features such as security, dependability, and performance. They offer secure over-the-air implementation via the OTA server, using transmission security, so outsiders cannot access update data. To verify the integrity and authenticity of the update kit, use a secure boot mechanism with cryptographic validation. It also has real-time monitoring or diagnostics, including engine telemetry and update state, to track update success and system health, allowing pre-emptive maintenance and problem estimation.

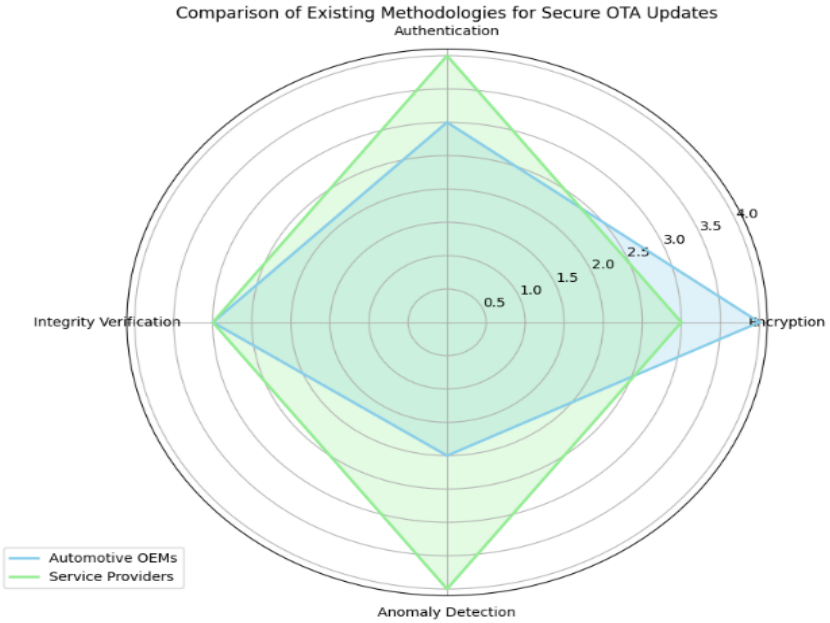

Figure 8: Secure OTA update Authentication

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

Source: Lienhard / Carlsson 2015 Based on Figure 8, it can be concluded that the various case studies and practical implementations have demonstrated the vast variety of approaches and technologies applied in the implementation of secure OTA updating process for connected vehicles. Thanks to the utilization of cutting-edge encryption, authentication, and monitoring measures, automotive manufacturers and service providers can guarantee the integrity, confidentiality, and reliability of the OTA update process, leading to improved safety, performance, and user experience of connected vehicles.

5.1 Automotive OEM Approaches

Table 1. OTA Update Approach

OEM	OTA Update Approach	Key Features
Tesla	Continuous OTA updates with scheduled release cycles	- Automatic download and installation
		- Differential updates for efficiency
		- Secure authentication and encryption
		- Rollback mechanisms for failed updates
BMW	Remote Software Upgrade platform	- Secure communication via HTTPS
		- End-to-end encryption
		- Incremental updates for bandwidth efficiency
		- Certificate-based authentication
Ford	Ford Power-Up OTA updates	- Remote deployment via cellular network
		- Secure boot process with cryptographic verification
		- Periodic security audits
		- User consent for update installation

5.2 Service Provider Solutions

Service providers also play a significant role in this field of secure over-the-air software updates for the connected car, offering OEMs and automobile manufacturers tailor-made solutions. Their technologies facilitate the deployment and management of over-the-air updates (OTAs) while establishing stringent security. Using their expertise in software management, cybersecurity, and networking, these service providers accommodate all the specific demands of the car industry by offering all-inclusive over-the-air update solutions.

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

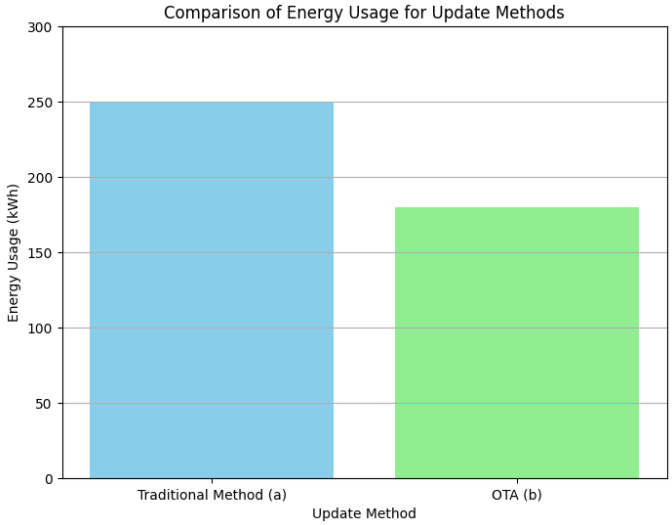

Figure 9: Comparison of Energy of OTA and Traditional methods

To deal with the intricacies and challenges of implementing car software upgrades, the top service providers such as Airbiquity, Continental, and Harman offer sophisticated over-the-air update management solutions . Firmware Over-The-Air Gateways and other protected communication channels enable encrypted update data transfer through cellular networks and additional communication are some frequent platforms. The role-based access control systems protect the confidentiality and integrity of the update process using authorized workers to restrict unauthorized access.

Table 2: OTA Update Solution

Service Provider	OTA Update Solution	Key Features
Airbiquity	OTAmatic ^⊖ OTA software and data management solution	- Secure data transmission via FOTA Gateway
		- Role-based access control
		- Integrity verification with digital signatures
		- Customizable update policies
Continental	OTA Connect ^⊕ solution for automotive OTA updates	- Secure over-the-air deployment via OTA server
		- End-to-end encryption
		- Secure boot process with cryptographic verification
		- Real-time monitoring and diagnostics

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

Harman	OTA update management platform for automotive systems	- Secure update distribution via OTA Cloud
		- Integrity checks and verification
		- Compliance with automotive cybersecurity standards
		- Real-time reporting and analytics

Additionally, in order to make absolutely sure that update packages are correct and contain no unauthorized modifications, service provider solutions also utilize integrity verification methods, including checksums and digital signatures . Real-time monitoring and pinpoint diagnostics of system performance and the update deployment process, along with any issues that arise as a function of the updates enhance the performance and reliability of over-the-air updates .

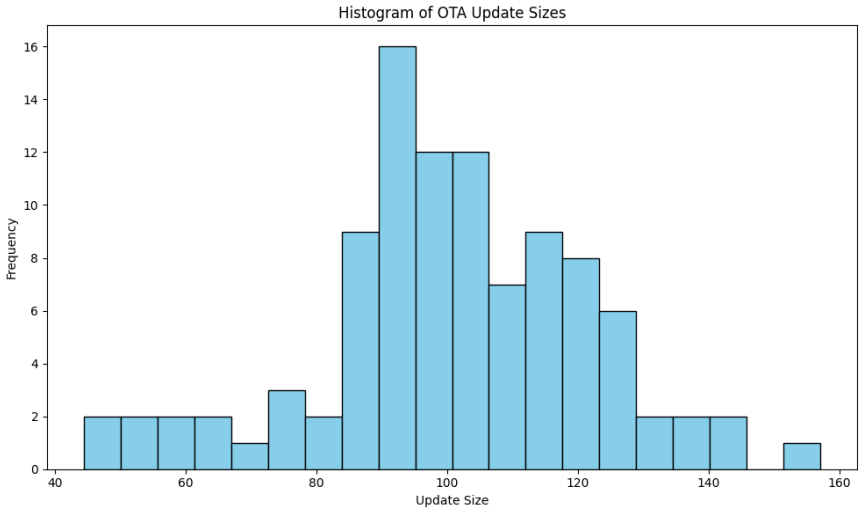

Figure 10: Histogram of OTA update size

To mitigate the posed potential security threats and risks, as well as the associated legal liabilities, attributed to over-the-air updates , service providers always ensure compliance with automobile cybersecurity standards and regulations, such as ISO 21434 and UN ECE WP.29 . Given that service provider solutions are continuously innovated and spectacularly enhanced to address new problems and advancements in automobility, the solutions will in due course allow automobile manufacturers to offer secure over-the-air updates. Manufacturers can collaborate with reputable service providers to create a secure, stable and efficient over-the-air update process to assure the long-term success of connected car ecosystems. This will provide optimal and adequate user experiences.

6. Future work and Conclusions

To close, it provides a new look in increasing the security of software updates for connected cars, which is accomplished via over-the-air transmission. The use of quantum-safe encryption is necessary to protect the over-the-air update system from threats that quantum computers will pose in the future. To guard against a quantum computer which may employ a legacy cryptographic approach, quantum-safe cryptographic algorithms were developed by developers. Manufacturers are able to take measures so that their over-the-air update system is future-proof by adopting quantum-safe encryption . Moreover, it is the practical advice contained in this document that makes sure updates conducted over-the-air are really secure. As the document recommends, all concerned should cooperate – from producers and sellers down to regulators. The document stresses the importance of abiding by sectoral and

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

rulemaking standards to ensure the safety and reliability of OTA update systems. In conclusion, the research will shap a future for the automotive industry which is more trustworthy, inventive, secure, and cybersecurity-proof at large in addition to just individual cars. Manufacturers of connected car technologies be able to instill confidence, promote innovation and prosper if they support the recommended framework on a globe which is increasingly interconnected.

References

[1] Fizza, K., Auluck, N., Azim, A., Maruf, M. A., & Singh, A. (2019, December). Faster ota updates in smart vehicles using fog computing. In Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion (pp. 59-64).

[2] Kim, G., & Jung, I. Y. (2019). Integrity assurance of OTA software update in smart vehicles. International Journal on Smart Sensing and Intelligent Systems, 12(1), 1-8.

[3] Halder, S., Ghosal, A., & Conti, M. (2020). Secure over-the-air software updates in connected vehicles: A survey. Computer Networks, 178, 107343.

[4] V. Roy. " An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.

[5] Kim, B., & Park, S. (2018, December). ECU software updating scenario using OTA technology through mobile communication network. In 2018 IEEE 3rd International Conference on Communication and Information Systems (ICCIS) (pp. 67-72). IEEE.

[6] Malik, A. W., Rahman, A. U., Ahmad, A., & Santos, M. M. D. (2022). Over-the-air software-defined vehicle updates using federated fog environment. IEEE Transactions on Network and Service Management, 19(4), 5078-5089.

[7] Hardik Agarwal, Kanika Somani, Shivangi Sharma, Prerna Arora , Puneet Singh Lamba, Gopal Chaudhary*, Palmprint Recognition Using Fusion of Local Binary Pattern and Histogram of Oriented Gradients, Fusion: Practice and Applications, Vol. 1 , No. 1 , (2020) : 22-31 (Doi : https://doi.org/10.54216/FPA.010103)

[8] Aditya Sharma , Aditya Vats , Shiv Shankar Dash , Surinder Kaur, Artificial Intelligence enabled virtual sixth sense application for the disabled, Fusion: Practice and Applications, Vol. 1 , No. 1 , (2020) : 32-39 (Doi : https://doi.org/10.54216/FPA.010104)

[9] Plappert, C., & Fuchs, A. (2023, December). Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles. In Proceedings of the 39th Annual Computer Security Applications Conference (pp. 268-282).

[10] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092

[11] V. Roy. " Breast cancer Classification with Multi-Fusion Technique and Correlation Analysis" Fusion: Practice & Applications, Vol. 9, No. 2, 2023 ,PP. 48-61.

[12] Wu, Z., Liu, T., Jia, X., & Sun, C. (2021, June). Security design of OTA upgrade for intelligent connected vehicle. In Proceedings of the 2021 1st International Conference on Control and Intelligent Robotics (pp. 736-739).

[13] Ghosal, A., Halder, S., & Conti, M. (2022). Secure over-the-air software update for connected vehicles. Computer Networks, 218, 109394.

[14] Khatun, M., Glaß, M., & Jung, R. (2021, February). An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle. In 2021 7th International Conference on Automation, Robotics and Applications (ICARA) (pp. 122-127). IEEE.

[15] Dakroub, H., & Cadena, R. (2014). Analysis of software update in connected vehicles. SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 7(2014-01-0256), 411-417.

[16] Chawan, A., Sun, W., Javaid, A., & Gurav, U. (2018). Security enhancement of over-the-air update for connected vehicles. In Wireless Algorithms, Systems, and Applications: 13th International Conference, WASA 2018, Tianjin, China, June 20-22, 2018, Proceedings 13 (pp. 853-864). Springer International Publishing.

[17] Plappert, C., & Fuchs, A. (2023, December). Secure and Lightweight ECU Attestations for Resilient Over-the-Air Updates in Connected Vehicles. In Proceedings of the 39th Annual Computer Security Applications Conference (pp. 283-297).

[18] Yeasmin, S., & Haque, A. (2021, September). A multi-factor authenticated blockchain-based ota update framework for connected autonomous vehicles. In 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) (pp. 1-6). IEEE.

[19] A. Sariga , J. Uthayakumar, Type 2 Fuzzy Logic based Unequal Clustering algorithm for multi-hop wireless sensor networks, International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 33-46 (Doi : https://doi.org/10.54216/IJWAC.010102)

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024

[20] Irina V. Pustokhina, Blockchain technology in the international supply chains, International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 16-25 (Doi : https://doi.org/10.54216/IJWAC.010103)

[21] Shavit, M., Gryc, A., & Miucic, R. (2007). Firmware update over the air (FOTA) for automotive industry (No. 2007-01-3523). SAE Technical Paper.

[22] Chowdhury, T., Lesiuta, E., Rikley, K., Lin, C. W., Kang, E., Kim, B., & Wassyng, A. (2018). Safe and secure automotive over-the-air updates. In Computer Safety, Reliability, and Security: 37th International Conference, SAFECOMP 2018, Västerås, Sweden, September 19-21, 2018, Proceedings 37 (pp. 172-187). Springer International Publishing.

[23] Mahmoud A. Salam , M.M.El-Gayar, A Novel Hybrid Bio-Inspiration Technique for Service Composition, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 05-14 (Doi : https://doi.org/10.54216/JCIM.000101)

[24] Hisham Elhoseny , Hazem EL-Bakry, Utilizing Service Oriented Architecture (SOA) in IoT Smart Applications, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 15-31 (Doi : https://doi.org/10.54216/JCIM.000102)

[25] Kexun, H., Changyuan, W., Yanyan, H., & Xiyu, F. (2020, June). Research on cyber security Technology and Test Method of OTA for Intelligent Connected Vehicle. In 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) (pp. 194-198). IEEE.

[26] Mahmood, S., Fouillade, A., Nguyen, H. N., & Shaikh, S. A. (2020, October). A model-based security testing approach for automotive over-the-air updates. In 2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW) (pp. 6-13). IEEE.

[27] Qureshi, A., Marvi, M., Shamsi, J. A., & Aijaz, A. (2022). eUF: A framework for detecting over-the-air malicious updates in autonomous vehicles. Journal of King Saud University-Computer and Information Sciences, 34(8), 5456-5467.

[28] Guissouma, H., Diewald, A., & Sax, E. (2019). A generic system for automotive software over the air (sota) updates allowing efficient variant and release management. In Information Systems Architecture and Technology: Proceedings of 39th International Conference on Information Systems Architecture and Technology–ISAT 2018: Part I (pp. 78-89). Springer International Publishing.

[29] Abdullah Ali Salamai, An Approach Based on Decision-Making Algorithms for Qos-Aware Iot Services Composition, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 08-16 (Doi : https://doi.org/10.54216/JISIoT.080101)

[30] Abedallah Zaid Abualkishik, Rasha Almajed, William Thompson, Intelligent Model for Customer Churn Prediction using Deep Learning Optimization Algorithms, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 43-54 (Doi : https://doi.org/10.54216/JISIoT.080104)

[31] Kornaros, G., Tomoutzoglou, O., Mbakoyiannis, D., Karadimitriou, N., Coppola, M., Montanari, E., ... & Gherardi, G. (2020). Towards holistic secure networking in connected vehicles through securing CAN-bus communication and firmware-over-the-air updating. Journal of Systems Architecture, 109, 101761.

[32] La Manna, M., Treccozzi, L., Perazzo, P., Saponara, S., & Dini, G. (2021). Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update. Sensors, 21(2), 515.

[33] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 ,PP. 42-52.

Doi : https://doi.org/10.54216/JCIM.140109
Received: January 02, 2024 Revised: March 22, 2024 Accepted: June 07, 2024