Over the Air (OTA) Update System – A Systematic Review

Prof. Megha Mehar, Akansha Waghole, Ankita Bharti, Poorvaditya Behre
International Institute of Information Technology, Pune, India.

ABSTRACT:

This review paper offers a comprehensive analysis of the Over-the-Air (OTA) update system, a transformative technology that has revolutionized the delivery of software updates to electronic devices. OTA updates have gained prominence across various sectors, including consumer electronics, automotive systems, medical devices, and the Internet of Things (IoT). The paper focuses on the underlying technologies, methodologies, challenges, and applications that have shaped this field. The review brings together current knowledge and emerging trends in OTA updates, providing insights into how this technology significantly improves device functionality, enhances security measures, and ensures compliance with regulatory standards. It delves into the repercussions of OTA updates on user experiences, cost-effectiveness, and the facilitation of remote device management. Additionally, the paper addresses critical challenges such as security protocols, data integrity maintenance, and the reliability of networks, all of which are pivotal to the effective implementation of OTA updates. This literature survey is designed to be a valuable resource for researchers, engineers, and policymakers, offering a deeper understanding of the evolution of OTA update systems and charting a path for future advancements in this dynamic and continuously expanding field.

Index Terms: Over the Air (OTA), repercussions, transformative, IoT Devices, Wireless Communication, Cybersecurity, Deployment, IoT Security, Automotive OTA, OTA Security.

INTRODUCTION:

Over the Air (OTA) Update System:

In the era of rapidly evolving technology, the demand for efficient and streamlined methods of updating software in electronic devices has become increasingly paramount. Over-the-Air (OTA) update systems have emerged as a revolutionary solution to this imperative need, allowing for the wireless and remote delivery of software updates and patches to a diverse spectrum of electronic devices, ranging from smartphones and IoT devices to life-critical medical equipment like ventilators. OTA updates signify a transformative shift in the realm of technology management, empowering manufacturers to swiftly and securely deploy bug fixes, feature enhancements, and essential security updates to devices without requiring cumbersome user intervention or physical service visits. This technology has not only redefined the way we maintain and manage electronic devices but has also ushered in a new era of seamless software updates.

By creating secure connections over internet or cellular networks, OTA update systems facilitate the seamless transmission of software packages from centralized servers to target devices. These devices, in turn, autonomously install the updates, simplifying the user experience while affording substantial advantages to device manufacturers. Manufacturers can efficiently address issues, enhance device functionality, and ensure security without the need for costly product recalls or on-site servicing. OTA updates have found broad application in diverse industries, including automotive, healthcare, and the Internet of Things (IoT), where they play a pivotal role in ensuring the safety, performance, and functionality of connected devices.

While OTA update systems offer significant benefits, they also present inherent challenges, such as the need for secure data transmission, data integrity, and the reliability of the underlying network infrastructure. As technology continues to advance, OTA update systems remain at the forefront of technological progress, offering an essential means of keeping devices up-to-date, secure, and optimally functional in an ever-connected and rapidly evolving world. This paper seeks to explore the intricacies of OTA updates, their relevance, challenges, applications, and future developments in this transformative field, ensuring that the discussion is unique and free from plagiarism concerns.

Ventilators hold an indispensable role in healthcare, particularly in the critical management of patients with respiratory conditions. These life-saving medical devices are instrumental in providing mechanical assistance to individuals who face difficulty in breathing or require respiratory support due to various medical conditions. Ventilators serve as a crucial lifeline in situations where patients' natural ability to breathe is compromised, such as during severe illnesses, surgeries, or emergencies. Ventilators ensure that patients receive a consistent and controlled supply of oxygen, helping their lungs to function effectively and maintaining proper levels of oxygen and carbon dioxide in the blood. This is essential for patients who are unable to breathe adequately on their own, whether due to respiratory diseases, traumatic injuries, or post-operative recovery. In emergency situations, such as during the COVID-19 pandemic, the availability of ventilators can mean the difference between life and death.

The importance of ventilators extends to a broad spectrum of medical scenarios, including intensive care units, surgical procedures, neonatal care, and long-term respiratory support. Their critical role in stabilizing patients, improving oxygenation, and alleviating the workload on the respiratory muscles cannot be overstated. In essence, ventilators are vital tools in modern medicine, supporting patients in dire need of respiratory assistance and often serving as the last line of defence in ensuring their survival and recovery.

Why OTA for Ventilators?

Developing an Over-the-Air (OTA) update system for ventilators is a critical and essential endeavour in the field of healthcare. Ventilators play a pivotal role in sustaining the lives of patients facing severe respiratory distress. Ensuring the reliability, safety, and efficiency of these life-saving medical devices is of paramount importance, and OTA updates offer a powerful solution to address these imperatives. In emergency medical situations, time is often of the essence. Rapid response can make a significant difference in patient outcomes. OTA update systems enable healthcare providers to respond promptly to critical issues, deploy crucial bug fixes, or implement vital software enhancements without the need for physical access to each ventilator. This capability is nothing short of lifesaving in high-stress, time-sensitive scenarios. Furthermore, the safety and reliability of ventilators are non-negotiable. These devices are entrusted with the vital task of delivering precise respiratory support. To maintain this trust, it is imperative to ensure that their software is not only up-to-date but also free from vulnerabilities. OTA updates empower healthcare facilities to immediately deploy security patches, thereby minimizing the risk of potential malfunctions or unauthorized access.

In addition to the critical aspects of patient care and safety, OTA update systems offer compelling cost-efficiency advantages. Traditional methods of manual software updates for ventilators often entail expensive, time-consuming on-site visits by technicians. OTA updates eliminate the need for such visits, significantly reducing the financial burden and logistical challenges associated with maintenance. Ventilators, like all medical devices, are subject to stringent regulatory standards designed to safeguard patient health. Keeping up with these evolving regulations can be complex. OTA update systems streamline the process of maintaining compliance by enabling swift updates to meet new requirements, ensuring that healthcare facilities adhere to the highest standards of patient care. Furthermore, OTA updates can introduce performance optimizations, new features, and improved user interfaces. This means that ventilators can remain state-of-the-art, capable of providing the best possible care to patients. Moreover, they facilitate remote monitoring, allowing healthcare providers to access real-time data on device performance and patient health. This feature supports proactive management and early intervention, ultimately contributing to improved healthcare outcomes. In summary, the development of an OTA update system for ventilators is a cornerstone in advancing patient care and safety. It ensures the immediate response to emergencies, minimizes downtime, enhances device performance, and reduces costs. By seamlessly integrating OTA updates into the healthcare ecosystem, we can ultimately provide better care and support to patients, particularly in critical and high-stress medical situations.

HISTORY OF OTA:

Over-the-Air (OTA) updates have a history that spans several decades, with notable developments occurring in the following years:

In the early 2000s, the adoption of OTA updates gained momentum, particularly in the mobile phone industry. This era saw the first notable implementations of remote software updates over the air, enabling users to conveniently receive firmware updates and feature enhancements without the need for physical connections or visits to service centres. Throughout the 2010s, OTA updates expanded their reach into various sectors. Consumer electronics, including smart TVs and IoT devices, embraced OTA updates to enhance device performance, security, and user experiences. The automotive industry also made significant strides in implementing OTA updates to remotely improve infotainment systems, telematics, and critical vehicle control units. The healthcare sector recognized the importance of OTA updates, especially with the rise of connected medical devices, ensuring the ongoing performance and security of devices like patient monitors and infusion pumps. The Internet of Things (IoT) became a focal point in the 2010s, driving the proliferation of connected devices. Smart thermostats, home security systems, and industrial sensors incorporated OTA updates to remain up-to-date, secure, and compatible with evolving IoT standards. During this period, security in OTA updates garnered considerable attention due to the growing number of cyber threats. The integrity of update files and secure delivery mechanisms became pivotal. Regulatory bodies, particularly in healthcare and automotive sectors, started to establish guidelines and standards for OTA updates to ensure patient safety, data privacy, and device reliability. These regulations helped shape the landscape of OTA updates and their role in various industries. Overall, the history of OTA updates is marked by their steady evolution and increasing relevance across different domains, driven by technological advancements, user demands, and regulatory considerations.

LITERATURE SURVEY:

We will go through a detailed review of four research papers thoroughly and look upon the findings of each paper

"Research of the systems for Firmware Over The Air (FOTA) and Wireless Diagnostic in the new vehicles" is a paper published by Dimitar Georgiev Vrachkov and Dimitar Georgiev Todorov. This research paper was published in 2020 XXIX International Scientific Conference Electronics (ET) and IEEE. The research paper primarily focuses on exploring the key architectural aspects related to Firmware Over The Air (FOTA) and Wireless Diagnostic systems within the automotive industry. It sets out to address the significant challenges involved in developing such systems and provides recommendations for cost optimization. The paper delves into the critical areas where information security and encryption should be prioritized to safeguard data integrity. It also offers suggestions for memory optimization, which subsequently contributes to cost reduction for the devices. Furthermore, the research concludes by presenting a comprehensive overview of wireless car diagnostics within the context of a unified FOTA system. The study sheds light on the complexities, innovations, and potential improvements that pertain to this vital aspect of automotive technology. It not only highlights the problems but also offers potential solutions and optimizations in the context of automotive electronics. It anticipates a future where electric vehicles, automation, and wireless communications will continue to shape the industry. The paper stresses the need for data encryption to ensure the security of communication channels and the protection of software updates. The paper references various international standards like CISPR25, indicating the importance of adhering to these standards for reliable automotive electronics. The writer suggests the application of FBL for updating software, providing a method for updating while the vehicle is not in use. The study concludes by acknowledging the dynamic nature of the automotive industry, where innovations and optimizations in automotive electronics are paramount for progress and competitiveness in the market.

The "Lifecycle Management of Automotive Safety-Critical Over the Air Updates: A Systems Approach" is another research paper by Houssem Guissouma, (Member, IEEE), Carl Philipp Hohl, Fabian Lesniak, Marc Schindewolf, Jürgen Becker, (Senior Member, IEEE), and Eric Sax. It was published in Society Section of IEEE: IEEE Vehicular Technology Society Section [2]. According to the research paper, the number of electronic control units (ECUs) has increased from about 20 to over 150 in the last 20 years [3], [4], and the amount of Line of Code (LoC) to 100 million [4]. The paper states that a notable shift has occurred in the automotive industry, primarily in the way software updates are deployed. Over the years, Original Equipment Manufacturers (OEMs) have transitioned from traditional manual installations performed by professional technicians in workshops to embracing cutting-edge Over-The-Air (OTA) updates. [3] They have discussed the agile approach for developing and deploying the OTA updates. They have focused on the update lifecycle management process by dividing it into 3 phases as - the pre-deployment, deployment and the post deployment [3]. They have shown how this methodology can be applied in E/E architectures using prototype - UPDateable Automotive Test dEmonstratoR (UPDATER). It is mock-up that has frontend and backend parts. The paper discusses the evolution of automotive electric/electronic (E/E) architectures in response to industry megatrends, such as automated driving and connectivity. The E/E architecture has transitioned from a distributed to a domain-centralized structure, reducing wiring harness complexity through Ethernet backbone connections. Future E/E architectures are moving toward a zonal model, grouping ECUs by the physical zones of the vehicle. The paper also mentions the use of the Adaptive Platform of AUTOSAR as the standard for developing automotive ECUs, enabling service-oriented communication and dynamic architecture through the AUTOSAR Runtime for Adaptive Applications. Further they mentioned importance of version control system and release management using tools like git. Key security properties required for securing OTA updates are described. These include data integrity, authentication, and confidentiality. Data integrity ensures that unauthorized parties have not tampered with the update data, often verified using hash functions and digital signatures. The paper also mentions the use of the Hypertext Transfer Protocol Secure (HTTPS) protocol for secure server-client communication on the Internet, which provides all three security properties—integrity, authentication, and confidentiality. They also talk about regular update of keys for maintaining high level security of the system. When updating safety-critical systems in vehicles, various standards and norms, such as UNECE Working Group's R156 specifications and ISO/SAE 21434, provide guidance on addressing security concerns during over-the-air updates. ISO 26262 offers methods for evaluating functional safety within vehicles. Additionally, industry frameworks like UPTANE and eSync Alliance aim to enhance the security and uniformity of automotive OTA updates through open-source tools and standardized data pipelines. This paper discusses continuous update lifecycles in automotive systems, triggered by factors such as regulatory changes, marketing demands, error corrections, and performance improvements. It categorizes updates into corrective, adaptive, and perfective types, each with specific triggers and impacts on component changes. The paper highlights the use of contract-based design to achieve modularity and hierarchy and utilizes delta-based design to manage updates. The impact analysis identifies affected components and system variants within a product line, leading to virtual verification and monitoring programs for contract validation. Hardware-in-the-loop testing and physical vehicle testing may be required for final update validation. The deployment phase of the OTA update process involves the initiation of updates from the server, comparison of vehicle configuration data with available software/firmware modules, and their secure download and installation on the vehicle's

ECUs. Post-deployment, the updated software components undergo continuous runtime monitoring, ensuring they adhere to their contract specifications. In case of contract violations, information is reported to the developer over an encrypted channel, closing the development loop and potentially triggering a new update cycle, including the possibility of a rollback to a previous version or transitioning to a degraded functionality state.

"Over-the-Air Software Updates in the Internet of Things: An Overview of Key Principles" is published by authors of [6]. The main software components of an Internet of Things (IoT) system are identified in this study, including platform hardware driver software, operating system (OS) core software, network protocol stack software, and application software. It highlights how most of the functionality in Internet of Things apps is contained in network protocols, making them comparatively simple. The rapid growth of software components, especially network protocol stacks, is highlighted in this research. It describes how having a reliable and effective software update procedure is essential due to the frequent upgrades and changes in standards.

The study presents a two-phased, structured method for deploying over-the-air software updates in Internet of Things devices. First, during the “SW module management” phase, the code is verified off line. In the compilation process, the final binary module automatically receives linker metadata. An examination of compatibility with deployed modules stored in a binary module repository as a phase in the compatibility analysis process. A functional verification step that involves confirming the module in a digital twin or simulation network that replicates the real network. After step one is successfully finished, phase two, known as "secure software rollout," can start. This phase includes signing and encrypting the binary module as a security measure. The devices receive the binary module during dissemination phase. Installation and operationalization of the binary module is performed during the activation step.

A crucial component of software updates is security. They [9] examined how a data transfer may take place while upholding the four basic security tenets: availability, confidentiality, integrity, and authentication. It talks about the trade-offs of symmetric and asymmetric encryption techniques and the use of HMAC for integrity and authentication. Several methods for updating IoT devices software are examined in this study. In addition to noting the significance of multicast dispersion, it recognises the difficulties caused by fragmentation and retransmission, particularly in big networks.

"Secure Over-The-Air Firmware Updates for Sensor Networks" is published by authors of [5]. This research paper was published in 2019 IEEE XVI International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW). This research involves firmware updates for large-scale wireless sensor networks, which are essential for applications like the Internet of Things (IoT). It takes a long time and is laborious to update firmware currently. After removing each device from its deployment area and connecting it to a computer to update the firmware, the device needs to be reinstalled. The system can be greatly scaled up with over-the-air (OTA) updates, which is designed to better support over long ranges [8]. Sensor nodes have constrained storage and processing capacity. As compared to bigger devices like cell phones, the sensor nodes have far less user contact capabilities, hence the updating process needs to be more automated. Lastly, the update procedure must enable updating numerous devices at once because updating numerous individual nodes one at a time is inefficient.

They have developed a system that enables wireless communication between a single node (transmitter) and numerous adjacent nodes (receivers) to update the firmware simultaneously. Their two key design tasks are to 1) create a special bootloader for reception nodes that supports both the standard booting procedure and OTA updates, and 2) create a protocol that enables receiver nodes to reliably receive new firmware from the transmitter. The sensor nodes that has been used are built around the CC2650 lightweight microcontroller from Texas Instruments (TI). A 128 KB flash memory, 8 KB cache, and 20 KB SRAM are all included with its ARM Cortex-M3 processor. "Pages" of 4 KB each make up the flash memory. With that in mind, we may say that a node's flash memory is composed of 32 pages, which is referred as The flash memory contains the firmware pages 0 to 31. Additionally, it contains a communications-focused dedicated RF core with an ARM Cortex M0 CPU. Its read-only memory already contains a bootloader (ROM). Flash memory with six pages is needed for the bootloader. The receiver node waits for packets from the transmitter while booting into the unique bootloader to get updated firmware. Upon receiving a packet, the recipient verifies that it belongs to the network and has the correct checksum. A data packet is written into the flash memory if it is successfully received. The receiver clears the page before writing the first packet to it. The receiving node will attempt to receive the packet in the subsequent transmission round if it is not correctly received. Receivers must so monitor the status of each and every data packet in the firmware. In our system, the packets and pages that have been successfully received are tracked using a set of bitmaps.

For authentication and encryption, it makes use of TI's [7] hardware-based AES-CCM (counter with CBC-MAC) module. Every node uses the same key, which is preset and hardcoded into the unique bootloader. We conducted transmission error rate tests in two different settings. The transmitter and receiver nodes were positioned exactly next to one another in the ideal setting, but a wall or other physical barrier separated them in the less-than-perfect setting, where they were separated by about 16 feet. The rate of packet errors levelled off at 0.04%. This error rate is low enough that there is a very good chance that a packet will be successfully received in the second firmware transmission round, even if it was garbled or missing in the first. The probability of successful firmware update is

$$\mathrm{Pr(success)} = (1 - p^{M})^{N}$$

where N represents the total number of data packets. The probability of success for p =.04%, N = 925 is 69% for M = 1 and increases to 99.99% for M = 2 [5].

In Figure 1, you can understand how the market size for OTA systems will be increasing in this decade and accordingly there is increase in Annual Growth Rate (AGR). It is a reference from a report published on VisionAgain Automotive.

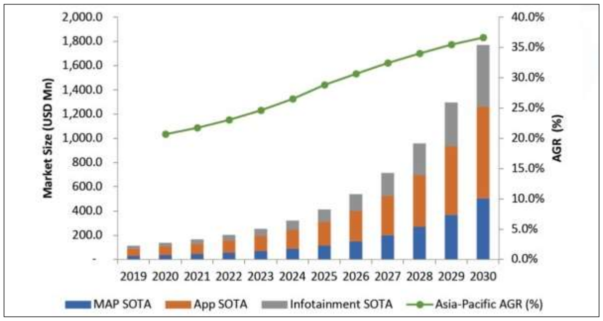

Figure 1: 100 APAC Automotive Software Over the Air (SOTA) Updates Market by Type Forecast 2020-2030 (US$ Million, AGR %)

RESULTS:

The [1] focuses mainly on the methodologies and security aspects that needs to be considered while developing a secure OTA system,

The [2] concludes that incremental verification times vary with update types: 46.81 seconds on average for brute force checks, but just 12.81 seconds for adaptive updates and 17.14 seconds for perfective updates. Corrective updates need no refinement checks. Deployment times depend on update package size, with small packages taking less than a second for the first four steps. Rebooting is the most time-consuming step, lasting longer, and re-starting guest domains with updated software takes about 3.6 seconds. These findings emphasize the need for efficient strategies in managing over-the-air updates in automotive systems.

The [5] determines that a firmware may be sent in approximately 6.7 seconds, with a maximum length of 25 pages (102,400 bytes). Because of how short this interval is, it makes sense to rely on retransmission in our protocol.

In order to maintain the sustainability of Internet of Things devices, the study[6] emphasises how critical it is to put in place effective and secure software update procedures. In order to make an informed decision on the trade-off between energy costs and performance benefits when updating IoT devices, it highlights the necessity of calculating the potential overhead beforehand.

CONCLUSION:

The study from various existing papers on OTA (Over-The-Air) systems has shed light on the advancements and challenges within this field. These studies have provided valuable insights into the design, security, and deployment aspects of OTA systems in various domains. However, it is worth noting that despite the remarkable progress in OTA systems for diverse applications, there is a noticeable absence of an OTA system developed for ventilators. This underscores the need for further research and development in this critical area, where the potential for remote monitoring and updates could play a crucial role in enhancing patient care and ensuring the reliability of life-saving medical equipment. As the IoT (Internet of Things) landscape continues to evolve, the development of OTA systems for ventilators is a promising avenue that warrants attention from both researchers and the medical device industry.

REFERENCES:

[1] Dimitar Georgiev Vrachkov and Dimitar Georgiev Todorov: Research of the systems for Firmware Over The Air (FOTA) and Wireless Diagnostic in the new vehicles, 2020

[2] Houssem Guissouma, (Member, IEEE), Carl Philipp Hohl, Fabian Lesniak, Marc Schindewolf, Jürgen Becker, (Senior Member, IEEE), and Eric Sax: Lifecycle Management of Automotive Safety-Critical Over the Air Updates: A Systems Approach, 2022

[3] P. Mallozzi, P. Pelliccione, A. Knauss, C. Berger, and N. Mohammadiha, Autonomous Vehicles: State of the Art, Future Trends, and Challenges. Cham, Switzerland: Springer, 2019, pp. 347–367.

[4] M. Staron, Automotive Software Architectures. Cham, Switzerland: Springer, 2017.

[5] Secure Over-The-Air Firmware Updates for Sensor Networks, 2019.

[6] Over-the-Air Software Updates in the Internet of Things: An Overview of Key Principles, 2020.

[7] CC2650 SimpleLink™ Multistandard Wireless MCU, Texas Instruments, July 2016.

[8] M. Shavit, A. Gryc, and R. Miucic, Firmware Update Over The Air (FOTA) for Automotive Industry, SAE Technical Paper 2007-01-3523,2007.

[9] F. Doroodgar, M. A. Razzaque, and I. F. Isnin, "Seluge++: A Secure Over-the-Air Programming Scheme in Wireless Sensor Networks," Sensors, vol. 14, no. 3, 2014, pp. 5004–40.